Inhalt

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

ARP	Address Resolution Protocol
CIFS	Common Internet File System
CPU	Central Processing Unit
DAS	Direct Attached Storage
DH-CHAP	Diffie-Hellman Challenge Handshake Authentication Protocol
DNS	Domain Name Service
DoE	Data over Ethernet
DoS	Denial of Service
DMZ	Demilitarisierte Zone
DHCP	Dynamic Host Configuration Protocol
ESP	Encapsulation Security Payload
FC	Fibre Channel
FCAP	Fibre Channel Authentication Protocol
FCPAP	Fibre Channel Password Authentication Protocol
FCsec	Fibre Channel Security
FC-SP	Fibre Channel Security Protocols
iSCSI	Internet SCSI
HBA	Host Bus Adapter
IOPS	Input/output operations Per Second
I/O-Pfad	Input/Output-Pfad
IP	Internet Protocol
IPsec	IP Security
K-Fall	Katastrophenfall
LUN	Logical Unit Number
MAC	Media Access Control
MITM	Man-In-The-Middle
NAS	Network Attached Storage
NFS	Network File System
OSI	Open Systems Interconnection Model
PCI	Peripheral Component Interface
RAID	Redundant Array of Independent Disks / Redundant Array of Inexpensive Disks
RADIUS	Remote Authentication Dial-In User Service

RSCN	Registered State Change Notifications
SAN	Storage Area Network
SAS	Serial Attached SCSI
(S)ATA	(Serial) Advanced Technology Attachment
SCSI	Small Computer System Interface
SMB	Server Message Block
SPT	Spanning Tree Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VM	Virtuelle Maschine
vFiler	Virtual Filer
VMFS	Virtual Machine File System
vSAN	Virtual Storage Area Network
WWN	Word Wide Name
WWNN	World Wide Node Name
WWPN	Word Wide Port Name

1 Einleitung und Übersicht

In der einleitenden Übersicht soll erläutert werden aus welcher Motivation heraus diese Arbeit entstanden ist und welches Ziel verfolgt wird. Zudem erfolgt eine Kapitelübersicht, aus der hervorgeht welcher und warum dieser Inhalt präsentiert werden soll.

1.1 Motivation

In den letzten Jahren haben viele Unternehmen die Virtualisierung von IT-Anwendungen und IT-Infrastrukturen[1] vorangetrieben, um damit die Grundlage für eine bedarfsgerechte IT zu schaffen. Die Virtualisierung von Serversystemen spielt dabei eine zentrale Rolle, denn sie ermöglicht unter anderem [Bitk2009]

- effiziente Ressourcennutzung,
- erhöhte Verfügbarkeit,
- Skalierbarkeit,
- schnelle Bereitstellung von IT Services,
- hohe Flexibilität/ Dynamik,
- vereinfachten Betrieb.

Spezielle Herausforderungen bestehen bei dem Aufbau von Virtualisierungsumgebungen im Bereich von DMZen[2] und der damit verbundenen Integration der Speichernetze[3]. Es besteht die Möglichkeit, dass durch eine nicht an die Virtualisierung angepasste Segmentierung des Speichernetzes Gefährdungen entstehen.

Es kann beispielsweise dazu kommen, dass virtuelle IT-Systeme den Zugriff auf, von ihnen benötigte, Ressourcen verlieren, wenn sie zwischen Virtualisierungsservern verschoben werden. Die Verfügbarkeit der von ihnen bereitgestellten Dienste ist damit gefährdet. Andererseits kann eine ungeeignete Planung der Speichernetzintegration dazu führen, dass zu weitreichende Zugriffsmöglichkeiten auf die Speichernetze eingeräumt werden. Dies kann die Vertraulichkeit von in diesen Speichernetzen abgelegten Informationen gefährden. [BSI2011]

---

[1] Virtualisierung bezeichnet in der Informatik die Erzeugung von virtuellen (nicht physikalischen) Instanzen, wie z.B. emulierter Hardware, Betriebssystemen etc.

[2] Eine DMZ ist ein durch Firewalls abgetrennter Netzwerk-Sicherheitsbereich mit eingeschränkten Zugriffsmöglichkeiten.

[3] Ein Speichernetz ist ein Netzwerk zur Anbindung von Speicherressourcen an Serversysteme.

Zudem hat die Anzahl der Angriffe aus dem Internet in den letzten Jahren stetig zugenommen. Die Delikte, die Datenveränderung und Computersabotage betreffen, haben sich in den letzten vier Jahren mehr als verfünffacht. Computersabotage beschreibt hierbei, im Sinne des deutschen Strafrechts, dass stören einer Datenverarbeitungsanlage, die für einen anderen von wesentlicher Bedeutung ist.

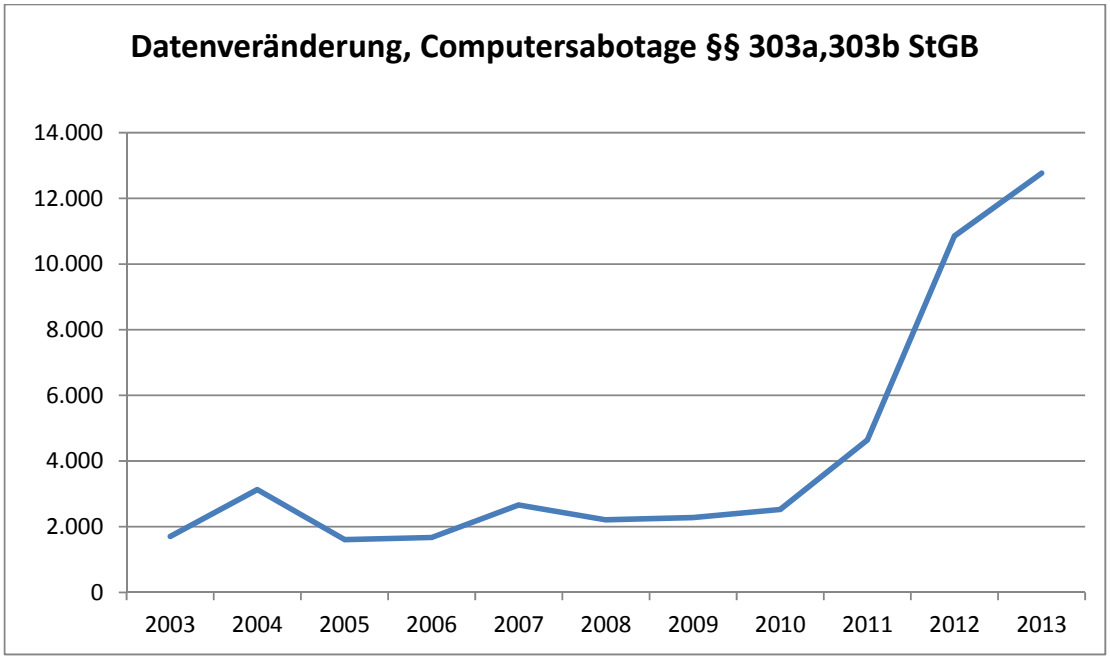

Abbildung 1: Computersabotage und Datenveränderung in Deutschland (BKA) [CoSa_2013]

Neben dem monetären Schaden der durch Computersabotage und Datenveränderung entsteht, sind die Folgeschäden, wie Imageverlust, schwer zu quantifizieren.

Da die Virtualisierung im Bereich von demilitarisierten Netzwerken, die direkt an das Internet grenzen, immer mehr zur Normalität wird, besteht auch ein immer größerer Bedarf für IT-Sicherheitsbeauftragte die Risiken und Auswirkungen, die mit dieser Praxis einhergehen, zu verstehen.

Die Arbeit ist aus der Motivation entstanden, unter vorgegebenen Rahmenbedingungen, unterschiedliche Speicherlösungen bezüglich Ihrer Integrationsmöglichkeiten und der damit verbundenen Risiken zu vergleichen und zu bewerten.

1.2 Zielsetzung

Die vorliegende Arbeit befasst sich im Rahmen der Aufgabenstellung mit der Gegenüberstellung verschiedener Speichernetze, die in Virtualisierungsumgebungen für x86[4]-Serversysteme eingesetzt werden.

Es werden unterschiedliche Integrationskonzepte für Speicherinfrastrukturen gegenübergestellt und unter anderem betrachtet welche Risiken vorhanden sind und welche Maßnahmen hinsichtlich der Authentifizierung und der Verschlüsselung, bei der Nutzung von Speichersystemen und Speichernetzen, notwendig sein können.

Zudem wird betrachtet welche Anforderungen bestehen, um verschiedene Sicherheitsklassen auf virtualisierten Umgebungen betreiben zu können.

So kann unter Umständen, je nach Unternehmensrichtlinie eine physikalische Trennung unterschiedlicher Sicherheitsklassen vorgeschrieben sein, um die Auswirkungen von Konfigurationsfehlern zu verringern.

Hauptziel ist eine Risikoklassifizierung, die unter Berücksichtigung spezifischer Parameter, für die jeweilige Referenzarchitektur, die möglichst beste Speicherlösung darstellt und als Entscheidungshilfe dient.

1.3 Kapitelübersicht

Die Diplomarbeit besteht aus acht Kapiteln.

Nach der allgemeinen Einleitung des ersten Kapitels wird im **Kapitel 2** die Abgrenzung der Aufgabenstellung durchgeführt. Hierbei wird dargestellt welche Problemkreise angesprochen werden und es wird abgegrenzt womit sich diese Arbeit auseinandersetzt.

Das Grundlagen **Kapitel 3** betrachtet die unterschiedlichen Speichernetze, die für die Themenbearbeitung relevant sind. Es werden deren Aufbau, protokollspezifische Eigenheiten und wichtige zusätzliche Dienste besprochen. Zudem werden die unterschiedlichen Segmentierungsmöglichkeiten betrachtet und erläutert. Außerdem werden im Grundlagenkapitel die, im weiteren Verlauf der Arbeit betrachteten, Referenzarchitekturen beschrieben. Das Kapitel 3 bildet das Grundlagenwissen für die folgenden Kapitel.

Das **Kapitel 4** stellt die möglichen Gefährdungen und Risiken, die durch Fehlkonfigurationen oder vorsätzliche schädigende Fremdeinwirkung entstehen können, für die jeweiligen Zielobjekte, wie Server, Switche und Speicher dar.

[4] x86 ist die Abkürzung einer Mikroprozessor-Architektur und der damit verbundenen Befehlssätze, welche unter Anderem von den Chip-Herstellern Intel und AMD entwickelt werden. [x86w2013]

Anschließend wird im **Kapitel 5** eine Risikowertung für die im Kapitel 4 ermittelten Gefährdungen durchgeführt, die es im Anschluss ermöglicht die Speicherlösungen miteinander zu vergleichen.

Im **Kapitel 6** wird die zusammenfassende Bewertung der einzelnen Speicherlösungen in Bezug auf die jeweilige Referenzarchitektur durchgeführt.

Kapitel 7 zeigt, unter den Aspekten der vorangegangen Kapitel, die Implementierung einer NAS- und SAN-Architektur, die höchsten Sicherheitsansprüchen genügt.

Das **Kapitel 8** fasst schließlich die Ergebnisse der einzelnen Kapitel der Diplomarbeit noch einmal zusammen und es wird ein Ausblick gegeben wie die Thematik vorgesetzt werden könnte.

2 Abgrenzung der Aufgabenstellung

Nach [Schm2009] lassen sich Speichernetze in drei Untergruppen einteilen:

- Direct Attached Storage (DAS)
- Storage Area Networks (SAN)
- Network Attached Storage (NAS)

Dabei ist es für die gängigsten virtuellen Maschinen vollkommen transparent auf welcher Art von Speichernetz diese abgelegt sind. Wobei alle drei Untergruppen ihre jeweiligen Vor- und Nachteile haben. Die Auswahl hierbei lässt sich nicht einfach in „gut“ oder „schlecht“ einteilen, sondern hängt von den konkreten Anforderungen ab. [VMWa2012]

Bei der vorliegenden Diplomarbeit wurde der Fokus auf die beiden Speichertechnologien gelegt, die sich in größeren Serverumgebungen etabliert haben (NAS, SAN mit Fibre Channel).

Hierzu ist unter Anderem die Marktanalyse von Gartner[5] für das Jahr 2012 zu beachten, die darstellt, dass NAS und Fibre Channel SAN den größten Marktanteil besitzen.

2011 Rank	2012 Rank	Access Protocol	2011 Revenue	2012 Revenue	Annual Growth Rate (%)	2012 Market Share (%)
1	1	NAS (NFS/CIFS)	4,509.5	5,227.7	15.9	64.2
2	2	Fibre Channel SAN	1,806.5	2,324.2	28.7	28.6
3	3	iSCSI SAN	484.5	588.9	21.5	7.2
-	**-**	**Total**	**6,800.6**	**8,140.8**	**19.7**	**100**

Tabelle 1: Gartner – Umsätze für Speichernetze nach Protokollen (in Mio. Dollar) [Ga2012]

[5] Gartner ist ein Marktforschungsunternehmen in der IT.

Da sich mit Direct-Attached-Storage keine hochverfügbaren bzw. K-Fall-sicheren Lösungen aufbauen lassen, wird es in dieser Diplomarbeit nicht weiter betrachtet. Zudem ist Direct-Attached-Storage fehleranfälliger und die vorhandene Festplattenkapazität wird schlechter ausgenutzt. Um nur einige weitere Punkte zu nennen. [DeIn2003] Es muss aber erwähnt werden, dass Implementierungen, basierend auf lokalem Speicher in einem verteilten Dateisystem, sich aktuell in der Entwicklung befinden (z.B. vSphere 5.5 vSAN-Feature) und DAS zukünftig wieder eine verstärkte Bedeutung erlangen könnte.

Der Schwerpunkt dieser Arbeit liegt bei einer sicherheitstechnischen Betrachtung und Bewertung. Selbstverständlich spielen bei der Auswahl von Speichernetzen und Speichertechnologien, für einen konkreten Einsatzfall, darüber hinausgehend noch weitere Punkte eine Rolle. Um nur Einige zu nennen sind hier Performance, Kostenlimits und Betriebskonzepte zu berücksichtigen. Die aber im Zuge der Eingrenzung des Themenfeldes, auf ein überschaubares Niveau, in dieser Arbeit nicht weiter betrachtet werden.

3 Grundlagen

Im folgenden Abschnitt soll versucht werden, die unterschiedlichen Arten von Speichernetzen zu erläutern und die wichtigsten Merkmale hervorzuheben.

Zudem werden die unterschiedlichen Integrationsmöglichkeiten von virtualisierten Servern in demilitarisierte Zonen dargestellt und exemplarisch einige Vor- und Nachteile genannt. Eine Wertung bzw. Festlegung auf die verwendete Integration findet hierbei nicht statt, da die Auswahl des gewählten Lösungsansatzes auch von den jeweiligen Sicherheitsrichtlinien eines Unternehmens abhängt und in den weiteren Kapiteln noch weiter betrachtet wird.

Das Grundlagenkapitel bildet die Basis für alle weiteren Betrachtungen.

3.1 Speichernetze

3.1.1 SAN-Storage

3.1.1.1 Aufbau

Bei SAN sind die Server über ein dediziertes Netzwerk, vergleichbar mit einem Backbone das ausschließlich Daten transportiert, an den Massenspeicher angeschlossen. Ein SAN ist ein sekundäres Netz das an das lokale Netz eines Unternehmens angrenzt. Die Server stellen hierbei die Verbindungsstelle dar. Dieses Netz kann mehrere Speichersysteme beinhalten, auf dass von einem oder mehreren Servern zugegriffen werden kann. Diese Zugriffe erfolgen blockbasiert, hierbei fordern die Rechner einzelne Datenblocks von einer Festplatte an.

Gewöhnlich wird ein SAN mit Fibre Channel[6] verbunden und in einer Switched Fabric betrieben. Die Switched Fabric ist eine Sternvernetzung, die durch Fibre-Channel-Switches realisiert wird. Um die Ausfallsicherheit zu erhöhen und auch Wartungen zu vereinfachen werden meist mehrere Switched Fabrics aufgebaut, die komplett voneinander unabhängig sind, aber trotzdem die gleichen Endgeräte an anderen Ports miteinander verbinden. [VMWa2012 S. 402]

[6] Fibre Channel ist die Bezeichnung einer seriellen Schnittstelle

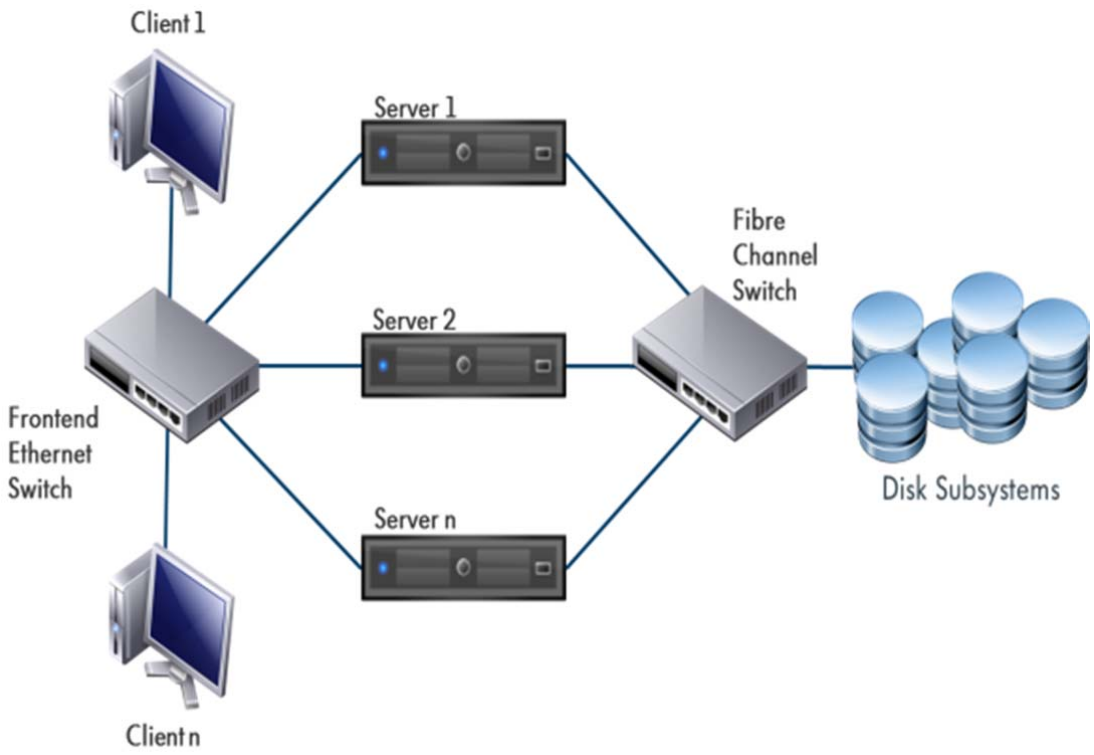

Abbildung 2: Blockdiagramm - Storage Area Network in einer Switched Fabric

Um in einem FC SAN betrieben werden zu können, müssen die Server, Speichergeräte und Switche mit einem oder mehreren Fibre-Channel-Ports ausgestattet sein. Bei Servern erfolgt der Anschluss in der Regel über sogenannte HBAs (Host-Bus-Adapter) die zusätzlich in die Server eingebaut werden. Hierbei werden folgende Ports unterschieden:

N-Port (Node-Port): Ein N-Port hat die Fähigkeit als Endgerät (Server, Speichergerät), auch Knoten genannt, in der Fabric-Topologie teilzunehmen.

F-Port (Fabric-Port): Ein F-Port stellt das Gegenstück zu einem N-Port dar. Der F-Port weiß wie ein Frame das ein N-Port an ihn sendet, durch das Fibre-Channel-Netz an das gewünschte Endgerät weitergeleitet werden muss.

E-Port (Expansion Port): Zwei Fibre-Channel-Switche werden über E-Ports miteinander verbunden. Die E-Ports übertragen hierbei die Daten von Endgeräten, die sich an unterschiedlichen Fibre-Channel-Switchen befinden. Zudem werden Switch Informationen über den Aufbau der Fabric ausgetauscht. [Spe2008]

Der Fibre-Channel-Standard definiert noch weitere Porttypen, z.B. in Zusammenhang mit anderen Topologien, auf die an dieser Stelle aber nicht weiter eingegangen wird.

3.1.1.2 Komponenten

Folgende Baugruppen beinhaltet ein SAN:

- Die Servern, die die Anfragen der Clients abarbeiten
- Die FC-Switches, die die Verbindung zwischen Servern und den Disksubsystemen herstellen
- Den Disksubsystemen, die als Speicherorte für die Daten dienen

3.1.1.3 IO-Pfad des Fibre Channel

Die Anwendungen und Anwender nutzen die Speicherkapazitäten der Festplatten in Form von Verzeichnissen und Dateien. Die physikalischen Blöcke der Festplatten werden hierbei durch den Volume Manager zu logischen Blöcken gruppiert und durch das Dateisystem den darüber liegenden Anwendungen bereitgestellt. [Spe2008] Verbreitete Dateisysteme im Zusammenhang mit Server-Virtualisierung sind das VMFS (Virtual Machine File System) von VMware oder das SMB (Server Message Block) von Microsoft. FCP (Fibre Channel Protokoll) bildet das SCSI-Protokoll, auf dass zugrunde liegende Fibre-Channel-Netz ab. Für die Anbindung von Speichergeräten an Server wird also das SCSI-Kabel durch ein Fibre-Channel Netz ersetzt. Das neue Medium Fibre Channel nutzt nach wie vor das SCSI-Protokoll, um Daten zwischen Server und Speicher auszutauschen. [Spe2008], S. 94

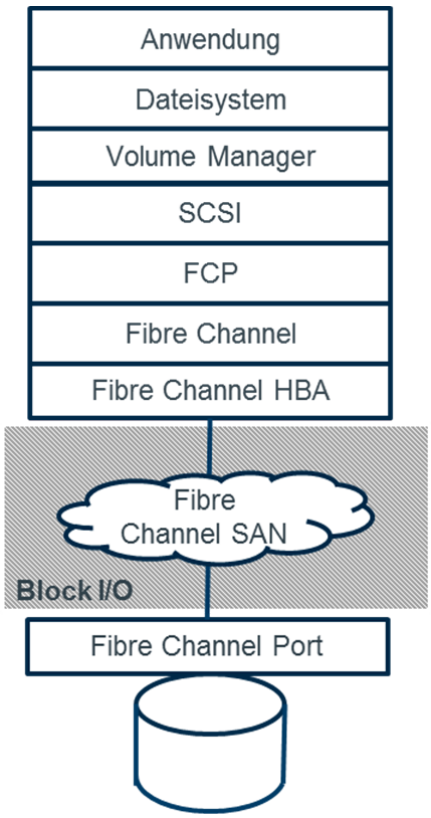

Abbildung 3: IO-Pfad des Fibre Channel

3.1.1.4 Datenübertragung

Das FC Protokoll führt eine dreischichtige Hierarchie zur Übertragung von Daten ein.

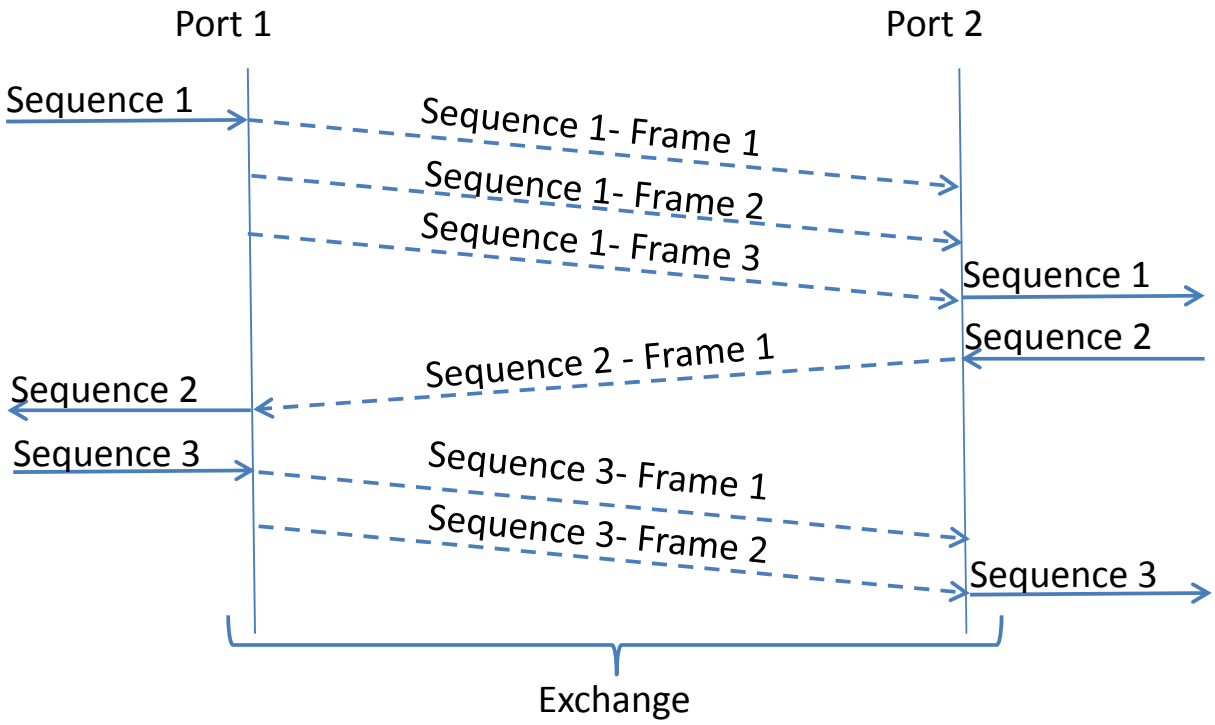

Abbildung 4: Datenübertragung bei Fibre Channel

Die oberste Ebene, der sogenannte Exchange, definiert eine logische Kommunikationsverbindung zwischen zwei Endgeräten. Server und Speichergerät können gleichzeitig mehrere Exchange-Beziehungen aufrechthalten, sogar zwischen den gleichen Ports.

Eine Sequence ist eine größere Dateneinheit, die von einem Sender zu einem Empfänger übertragen wird. Innerhalb eines Exchange kann nur eine Sequence nach der anderen übertragen werden. Eine Sequence wird nur dann an die nächsthöhere Protokollschicht ausgeliefert, wenn alle ihre Frames beim Empfänger angekommen sind.

Im Fibre-Channel-Netz werden Kontroll-Frames und Datenframes übertragen. Die Kontroll-Frames enthalten hierbei keine Nutzdaten, signalisieren z.B. aber das erfolgreiche Ausliefern eines Datenframes. Die Datenframes hingegen übertragen bis zu 2112 Byte Nutzdaten. Größere Sequences müssen deshalb auch in mehrere Frames unterteilt werden.

Fibre Channel Frames bestehen aus einem Header, Nutzdaten (Payload) und einer CRC-Prüfsumme. Zudem wird das Frame von einem Start-of-Frame Delimiter (SOF) und einem End-of-Frame Delimiter (EOF) eingerahmt. Als Abschluss werden über einen Link zwischen zwei Frames sechs Füllwörter übertragen. [Spe2008]

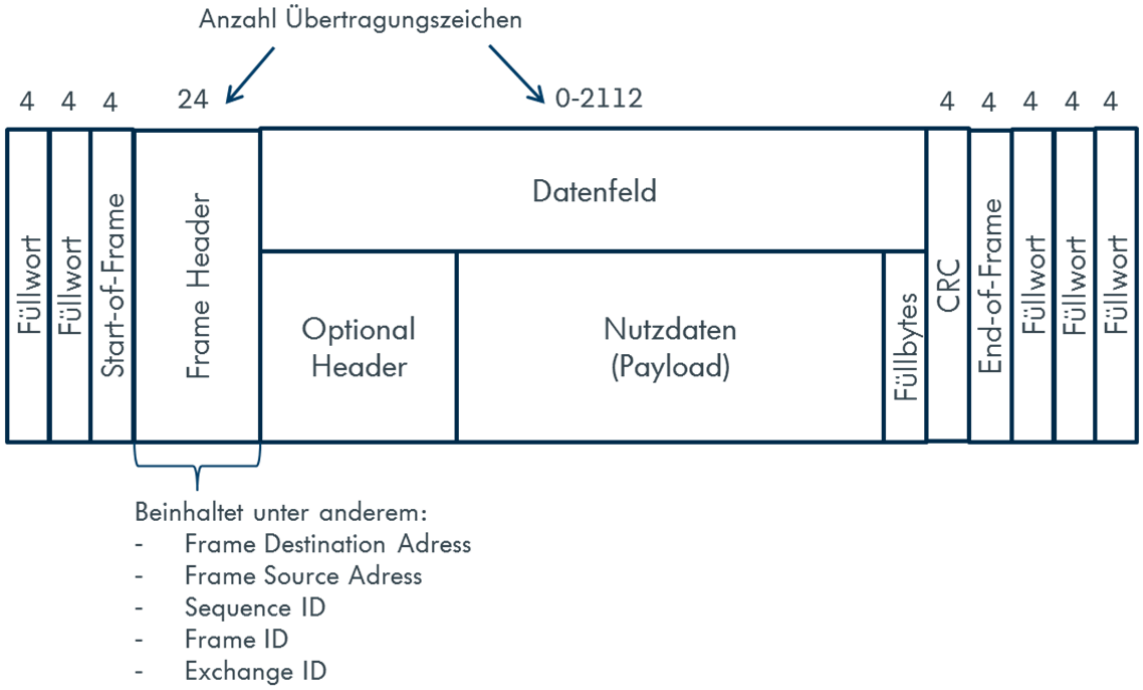

Abbildung 5: Fibre-Channel-Frame-Format [Spe2008]

3.1.1.5 Link und Fabric Services [Spe2008]

Die Link Services werden benötigt, um in einem Fibre-Channel-Netz Datenverkehr zu ermöglichen. Sie dienen der Verwaltung des Fibre-Channel-Netzes und ermöglichen somit den Datenverkehr auf Anwendungsprotokollebene.

Login

Bevor Anwendungsprozesse Daten austauschen können, müssen sich die beiden zur Kommunikation vorgesehen Ports miteinander bekanntmachen. Ein dreistufiger Login-Mechanismus ist hierfür durch den Fibre-Channel-Standard vorgesehen.

1. Fabric Login (FLOGI)
   Nach dem Initialisieren des Link findet das Fabric Login statt das eine Sitzung zwischen einem N-Port und einem gegenüberliegenden F-Port etabliert. Der N-Port weist dem F-Port hierbei 24-Bit-Portadresse zu und außerdem wird der Buffer-to-Buffer-Credit[7] ausgehandelt.

2. N-Port Login (PLOGI)
   Nach dem Fabric Login findet das N-Port Login statt. Hierbei wird eine Sitzung zwischen zwei N-Ports aufgebaut. Es ist die zwingende Voraussetzung für den Datenaustausch und definiert Service-Parameter wie den End-to-End Credit.

[7] Der Buffer-to-Buffer Credit definiert zwischen den beiden Endpunkten die Anzahl von Paketen die im Eingangspuffer Platz finden.

3. Process Login (PRLI)
   Der Fibre-Channel-Login-Mechanismus wird mit dem Prozess-Login abgeschlossen und definiert die Sitzung zwischen zwei Prozessen, die auf zwei verschiedenen N-Ports aufsetzen.

Adressierung

Bei Fibre Channel wird zwischen Adressen und Namen unterschieden. Die Fibre Channel-Geräte wie Server, Switche und Ports werden durch eine 64-Bit-Kennung gekennzeichnet. Hierzu sind verschieden Namensformate definiert, die gewährleisten, dass Kennungen weltweit nur einmal vergeben werden. Diese Kennungen tragen deshalb auch den Namen World Wide Name (WWN).

Die WWNs werden zudem noch unterschieden in World Wide Port Names (WWPNs) und in World Wide Node Names (WWNNs). Dem Fibre Channel Gerät wird der Word Wide Node Name, seinen Fibre Channel Ports der World Wide Port Name zugeordnet. Diese Unterscheidung ermöglicht es festzustellen, welche Ports zu einem gemeinsamen Multi-Port-Gerät gehören.

Beim Fabric Login wird jedem 64-Bit World Wide Port Name eine 24-Bit Portadresse zugeordnet. Diese 24-Bit Portadresse wird innerhalb der Fibre Channel Frames zur Sender- und Empfängerkennzeichnung genutzt. Die 24-Bit Port-Adressen sind hierbei hierarchisch aufgebaut (je 8-Bit Domain Name, Area Name, Port Name), sodass ein FC Switch einfach ableiten kann, an welchen Port er ein eintreffendes Paket weiterzuleiten hat.

Name Server

Der Name Server verwaltet eine Datenbank über N-Ports. Es werden unter anderem Informationen über World Wide Port Names (WWPNs), World Wide Node Names (WWNNs), Port-Adressen, unterstützende Dienstklassen etc. gespeichert. Beim Name Server können N-Ports ihre eigenen Attribute registrieren und Informationen über andere N-Ports abfragen, vorausgesetzt sie haben sich mittels Port Login bei Ihm eingeloggt. Der Name Server erscheint den anderen Ports selbst als N-Port.

3.1.1.6 Segmentierung / Zugriffsteuerung

Die Segmentierung in Storage Area Networks erfolgt durch Zoning und LUN Masking. Ohne diese Mechanismen würde die Segmentierung auf IP-Ebene zunichte gemacht werden und ein einzelner kompromittierter Server hätte Zugriff auf das komplette SAN.

Zoning stellt hierbei die Zugriffssteuerung auf Ebene des Speichernetzes und das LUN-Masking die Zugriffssteuerung auf Ebene des Speichersystems dar.

Zudem unterstützen neuere FC-Switche auch die Bildung von Virtual Storage Area Networks.

Virtual SAN (VSAN)

Ein Virtual SAN ermöglicht es über ein physikalisches Fibre Channel SAN mehrere virtuelle Fibre Channel Fabrics zu betreiben, die logisch voneinander getrennt sind. [Spe2008] S.511

Hierzu werden entweder die Ports der Fibre-Channel-Switche jeweils einem vSAN fest zugeordnet oder die Zuordnung erfolgt an Hand von WWNs. Die vSANs arbeiten vollkommen autark voneinander, sind erweiterbar, unterstützen eigene SAN-Services wie Zoning und Name Service und verfügen über eigene Sicherheitskriterien. [CSSE2011]

Zoning

Zoning erlaubt eine Segmentierung von Netzelementen, wie Speichersystemen, Switches und Host-Bus-Adaptern. Die Sichtbarkeit der Ressourcen für die Netzteilnehmer wird auf die freigegebenen Ressourcen beschränkt. Alle nicht gezonten Kommunikationswege werden ausgeblendet. [CSSE2011] Dies kann auf unterschiedlichen Wegen erfolgen.

Hard Zoning
Bei Hard-Zoning können nur diejenigen Endgeräte miteinander kommunizieren, die mindestens in einer gemeinsamen Zone liegen. [Spe2008] S.493

Soft Zoning
Soft-Zoning beschreibt eine Zoning-Variante, die sich auf die Auskunft des Name Servers beschränkt. Befragt ein Endgerät den Name Server nach anderen Endgeräten im Fibre-Channel-Netz, so bekommt es nur die Endgeräte mitgeteilt, mit denen es mindestens in einer gemeinsamen Zone liegt. Kennt ein Endgerät allerdings die Adresse eines anderen Geräts, mit dem es nicht in einer gemeinsamen Zone liegt, so kann es trotzdem mit dem anderen Gerät kommunizieren. [Spe2008], S.507

Die Identifikation der Netzelemente erfolgt entweder auf Basis von WWNs (Word Wide Numbers) oder die Port-Adressen an denen die Netzteilnehmer angeschlossen sind (Port-Based). [Spe2008]

LUN-Masking

Der Zugriff auf die durch das Disksubsystem präsentierten Festplatten wird durch das LUN Masking beschränkt. Ohne LUN Masking würde jeder Server alle Festplatten sehen, die das Disksubsystem bereitstellt. Dabei werden die innerhalb eines Disksubsystems nach außen hin sichtbaren Festplatten einzelnen Servern zugeordnet und somit die Sichtbarkeit von exportierten Festplatten eingeschränkt. Die Maskierung wirkt als Filter zwischen den nach außen geführten Festplatten und den darauf zugreifenden Rechnern und kann vom Server, Switch oder Speichersystem durchgeführt werden. [Spe2008]

3.1.2 NAS-Storage

3.1.2.1 Aufbau [BSI2014]

Ein NAS-Server stellt einen vorkonfigurierten Datei-Server dar, der seine Speicherkapazitäten über Ethernet zur Verfügung stellt. Hierbei kann sich der Massenspeicher im selben IP-Netz wie die Clients oder, wie in Abbildung 3 dargestellt, in einem separaten DoE[8]-Netz befinden.

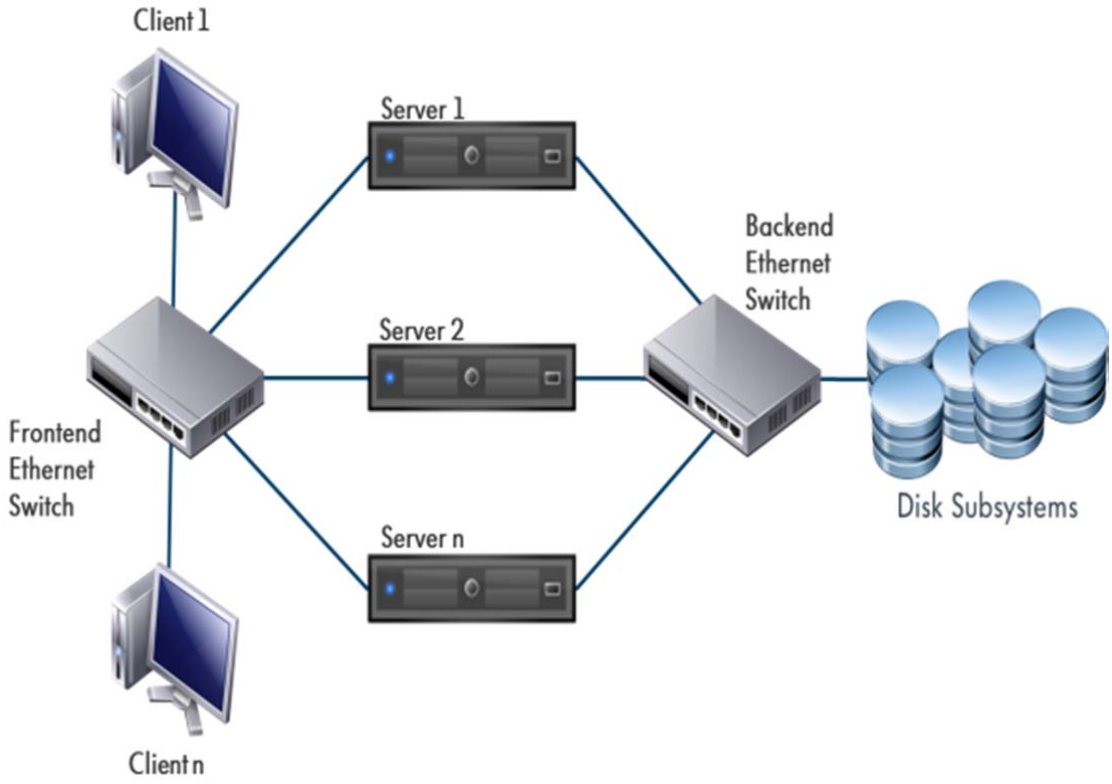

Abbildung 6: Blockdiagramm - Network Attached Storage

Im Gegensatz zu einem SAN, erfolgt die Datenübertragung in einem NAS auf Dateiebene. NAS-Systeme besitzen hierzu Echtzeitbetriebssysteme die auf den Dateitransfer ausgelegt sind und nutzen unter anderem die Protokolle NFS, CIFS oder SMB.

3.1.2.2 Komponenten

Folgende Baugruppen beinhaltet ein NAS:

[8] Ein DoE –Netz (Data over Ethernet) ist ein dediziertes IP-basiertes Netz in dem nur mit Speicherprotokollen kommuniziert wird.

- Die Server, die die Anfragen der Clients abarbeiten.
- Die Ethernet-Switches, die die Verbindung zwischen Servern und den NAS-Servern herstellen.
- Die NAS Servern, die als Speicherort für die Daten dienen.

3.1.2.3 IO-Pfad des NAS

Wie beim SAN nutzen die Anwendungen und Anwender die Speicherkapazitäten der Festplatten in Form von Verzeichnissen und Dateien. Der NFS Client baut eine TCP/IP-Netzwerkverbindungen zum NFS-Server auf. Der NFS-Server greift auf die, durch das Dateisystem bereitgestellten, Daten zu. Unterhalb des Dateisystems werden die physikalischen Blöcke, wie beim SAN, durch den Volume Manager zu logischen Blöcken gruppiert und anschließend wird über das SCSI Protokoll, den SCSI-Bus und den SCSI-HBA auf die Festplatten zugegriffen.

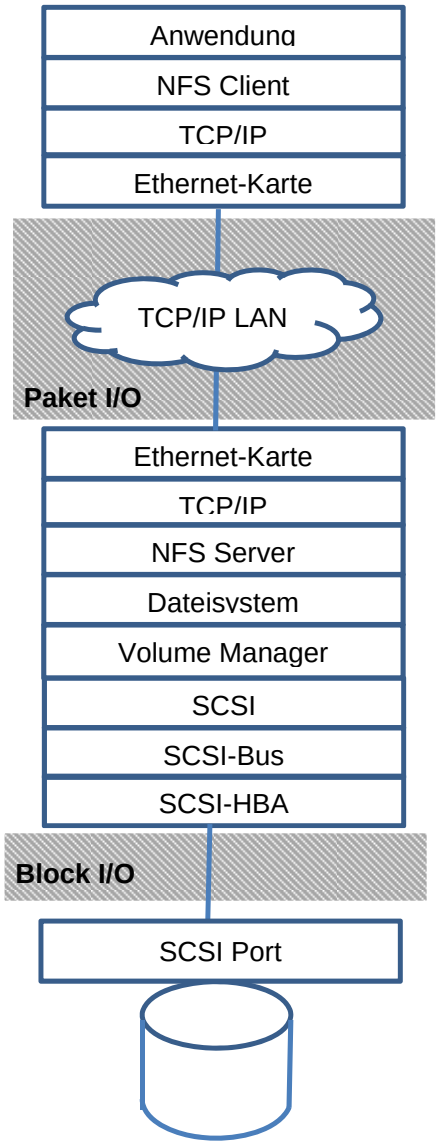

Abbildung 7: I/O-Pfad des NAS mit SCSI

3.1.2.4 Datenübertragung [Int22012]

Abbildung 8 stellt NAS-Systeme innerhalb des OSI-Modells dar. Hierbei ist die Unterteilung in folgende Protokolle und Dienste möglich.

- Kernprotokolle wie UDP/ TCP; IP
- Helferprotokolle wie ICMP, ARP, DHCP, DNS
- und Helferdienste wie DHCP, DNS

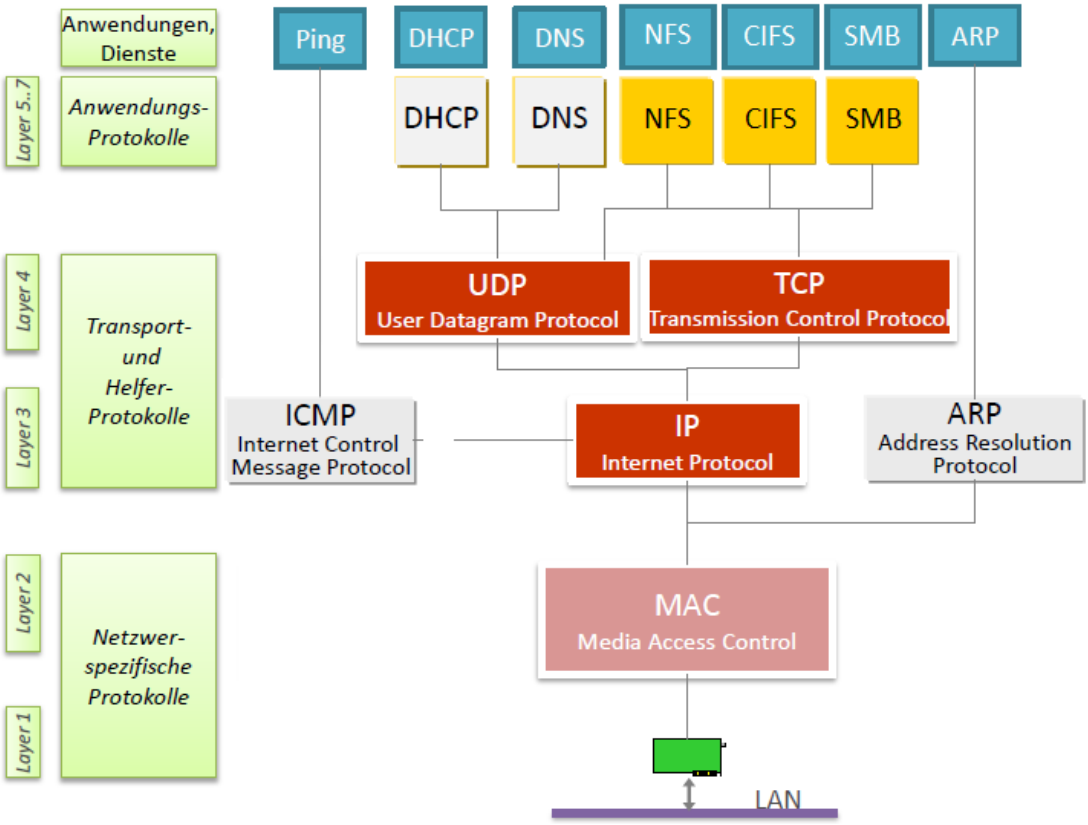

Abbildung 8: Kerntransportprotokolle [Int22012] S.5

Die Datenübertragung lässt sich nach dem OSI-Modell abstrahieren. Folgender Protokollstack wird hierbei verwendet.

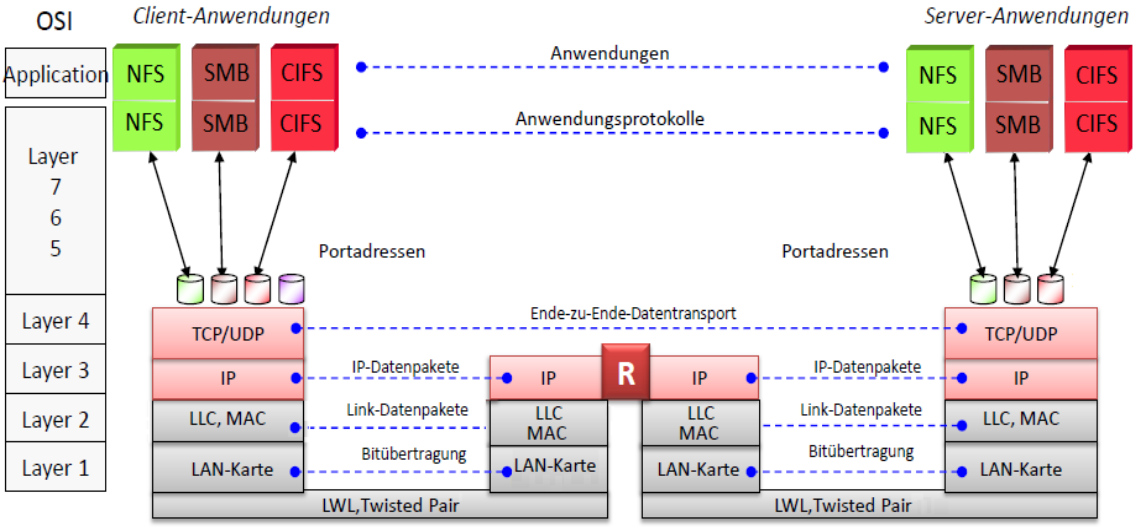

Abbildung 9: OSI Sicht NAS-Protokollstack [Int22012] S.4

Auf Schicht 1 findet die Datenübertagung auf Bit-Ebene statt.

Die Schicht 2 definiert die Datenübertragung über „Links“. Adressiert werden die Datenpakete hierbei über die MAC-Adressen. Diese ist 48-Bit lang und weltweit eindeutig (vergleichbar mit den WWNs im SAN). In der Regel sind die MAC-Adressen auf den Netzwerkkarten fest gespeichert, wobei einige Hersteller das Überschreiben zulassen.

In der Schicht 3 findet die Datenübertragung über das IP-Protokoll statt. IP ist verbindungslos, dass bedeutet, dass die Datenpakete vom Empfänger nicht quittiert werden. Große Datenpakete werden fragmentiert und erst am Ziel wieder zusammengesetzt. Das Routing findet dabei anhand der IP-Adresse statt. Sollten Fehler in der Netzschicht auftreten werden diese über das Internet Control Message Protocol (ICMP) der Quelle mitgeteilt.

Schicht 4 wird durch das Transmission Control Protocol (TCP) und das User Datagram Protocol (UDP) genutzt.

TCP wird als hoch verlässliches Host-zu-Host Protokoll in paketvermittelnden Computernetzen verwendet.

Der Verbindungsaufbau, vor der Datenübertragung, findet zwischen den beiden TCP-Instanzen in einem 3-Wege-Handshake Verfahren statt. Hierbei handelt es sich um eine Duplex-Verbindung, bei der jede Seiten einen Bytestrom zur anderen Seite sendet.

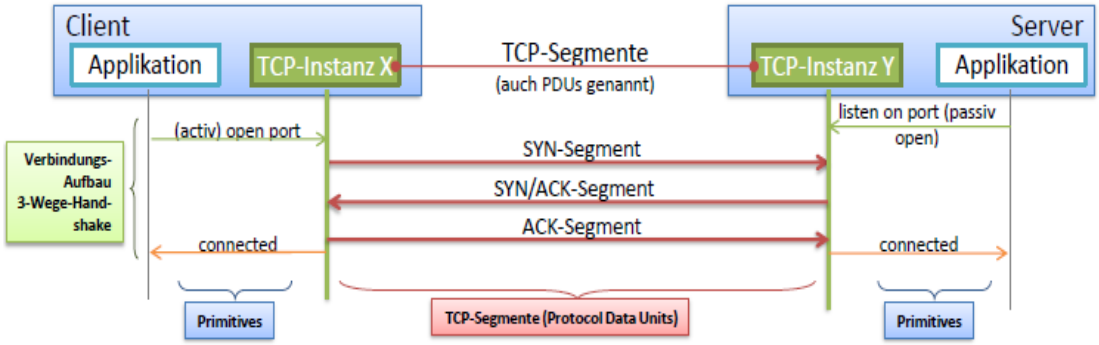

Abbildung 10: Funktionsweise TCP-Verbindung [Int22012] S.40

Für die Datenübertragung werden die Daten segmentiert und jedes Segment mit einem Header versehen.

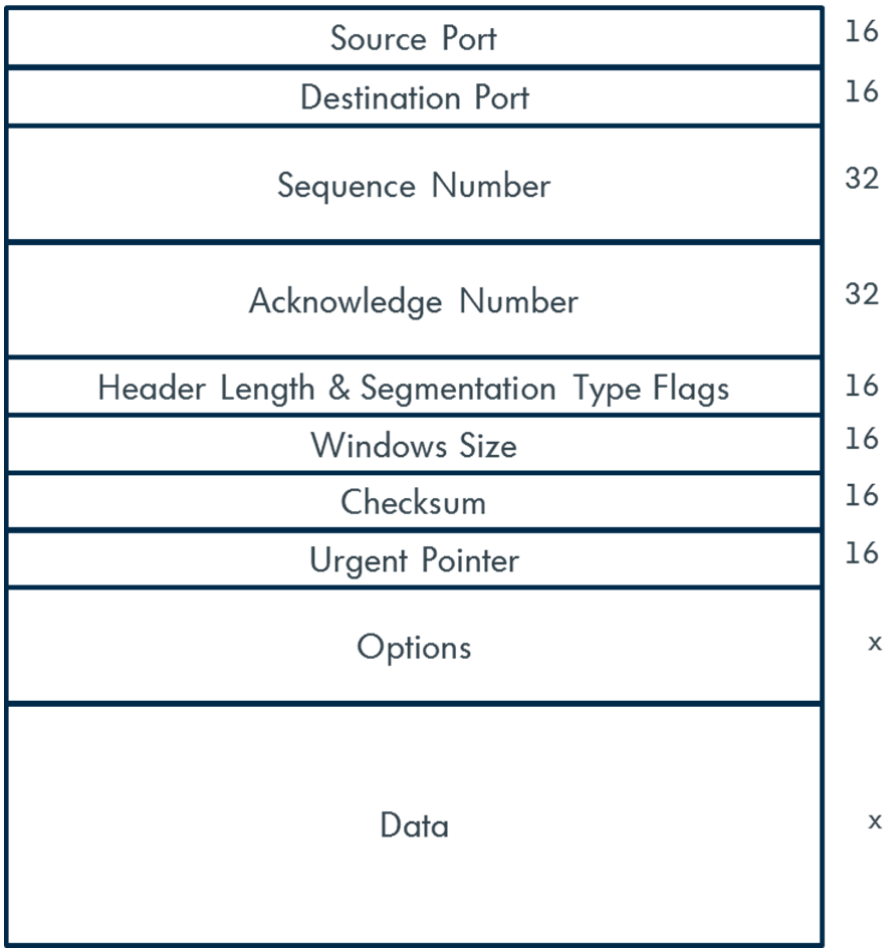

Abbildung 11: TCP - Protocol Informationen

Das TCP Protokoll verfügt über den obig dargestellten Aufbau.

Über den **Source**- und **Destination Port** findet die Bindung der Anwendungen an den TCP Stack statt. Mittels der **Sequence Number** werden die Datenpakete nummeriert. Dies ist die Voraussetzung für die Erkennung fehlender Pakete. Die **Acknowledge**

Number wird zur Quittierung des Startwertes bzw. der Daten verwendet. Die **Header Length** beschreibt die Länge des Headers, während die **Segmentation Type Flags**, den Typ des TCP Pakets kennzeichnen. Die Größe des Empfangspuffers wird mittels der **Windows Size** übertragen und die **Checksum** dient der Fehlererkennung. Abschließend werden **Optionen** und **Daten** übertragen (falls vorhanden).

3.1.2.5 Helferprotokolle und Helferdienste

Den folgenden Helferprotokollen und -diensten wird bei sicherheitstechnischen Betrachtungen verstärkt Aufmerksamkeit gewidmet, deshalb werden diese im Anschluss kurz erläutert.

Address Resolution Protocol (ARP) **[TdI2007]**

Bei ARP handelt es sich um ein Netzwerkprotokoll, dass die Zuordnung von Internet-Adressen (IP-Adressen) zu Geräteadressen (MAC-Adressen) ermöglicht und zur IP-Netzwerk-Protokollfamilie gehört. Das Address Resolution Protocol ermöglicht die Übertragung von Ethernet-Frames auf dem Niveau der Netzwerkschicht mit dem Internetprotokoll.

Domain Name Service (DNS) [Int12012]

Die Aufgabe des Domain Name Service ist die Abbildung von Host-Namen auf IP-Adressen. Anfangs hatte jeder Host die „Hosts“ Datei in der die Zuordnung abgebildet war. Heutzutage wird die Zuordnung mit dem Domain Name Service realisiert, der eine verteilte, hierarchisch Organisierte Datenstruktur darstellt.

Spanning Tree Protocol (STP) [Int12012]

Zur Erhöhung der Zuverlässigkeit werden LANs u.U. durch zwei oder mehr Bridges miteinander gekoppelt. Durch diese Kopplung können im Netzwerk Schleifen entstehen, die zum Fluten des Netzwerkes führen können. Um solch ein Verhalten zu vermeiden, verfügen Bridges über den Spanning Tree Algorithmus. Dieser lässt zwischen LANs nur einen aktiven Weg zu und ermöglicht im Fehlerfall des aktiven Weges einen Ersatzweg.
Nach dem Einschalten der Bridges sind alle ihre Ports gesperrt. Dann sendet jede Bridge „Bridge Protocol Data Units“ (BPDUs) mit ihrer jeweiligen ID aus. Die Brücke mit der kleinsten ID ernennt sich zur Root-Bridge und versendet Konfigurations-BPDU’s und initiiert somit die Netzkonfiguration und Freischaltung der Pfade.

Dynamic Host Configuration Protocol (DHCP) [Int12012]

DHCP stellt das Grundgerüst für die Übertragung von Konfigurationsinformation über TCP/IP Netzwerke zur Verfügung. DHCP basiert auf dem Bootstrap Protocol (BOOTP),

mit den ergänzenden Fähigkeiten der automatischen Zuordnung von wiederverwendbaren Netzwerkadressen und zusätzlichen Konfigurationsoptionen.

3.1.2.6 Segmentierung / Zugriffssteuerung

Die Segmentierung und Zugriffsteuerung bei NAS-Speicher beinhaltet TCP-IP und zusätzliche NAS-Technologie und -Protokoll spezifische Sicherheitsmechanismen.

VLAN

Ein Virtual Local Area Network (VLAN) ist ein logisches Teilnetz innerhalb eines Switches oder eines gesamten physischen Netzes. Ein VLAN kann sich hierbei über ein ganzes geswitchtes Netz hinziehen und braucht nicht nur auf einen einzelnen Switch beschränkt zu bleiben. Ein VLAN trennt physische Netze in Teilnetze auf, indem es dafür sorgt, dass VLAN-fähige Switche, Frames (Datenpakete) eines VLANs nicht in ein anderes VLAN weiterleiten. Dies gilt auch, wenn die Teilnetze an gemeinsame Switches angeschlossen sind. Ein VLAN bildet gleichzeitig eine separate Broadcast-Domäne. Das bedeutet, dass Broadcasts nur innerhalb des VLANs verteilt werden. [CSSE2011]

vFiler

Die vFiler ermöglichen isolierte logische Partitionen auf einem einzigen Disksubsystem. Somit wird der Zugriff nicht autorisierten Benutzern auf Informationen aus einer sicheren virtuellen Partition unterbunden. Zudem ermöglicht die Virtualisierung der Filer[9] eine Migration dieser zwischen den Storagesystemen und erleichtert dadurch die Wartbarkeit.

Authentifizierung

Die Authentifizierung erfolgt bei NAS oft ausschließlich anhand der IP-Adressen. Ein NAS-Filer der das CIFS Protokoll einsetzt, kann durch Verwendung der New Technology Local Area Network Manager Version 2 (NTLMv2) oder Kerberos Authentifizierungsmechanismen abgesichert werden. Ein NAS-Filer der das NFS Protokoll einsetzt, kann durch Verwendung des Kerberos Authentifizierungsverfahren abgesichert werden.

3.2 Speicherarchitekturen in DMZen [VMWa2014]

Mit einem steigenden Grad der Virtualisierung spielt auch die Integration in demilitarisierte Zonen eine immer größere Rolle, um möglichst hohe Virtualisierungsgrade zu erzielen. Es gibt hierbei verschiedene Ansätze von „leichter“ Virtualisierung bis hin zu „kompletter“ Virtualisierung. Einige verschiedene Möglichkeiten sollen im Folgenden veranschaulicht

[9] Filer ist die Bezeichnung eines Dateiservers, der für hohen Datendurchsatz, Backup und Archivierung optimiert ist.

werden. Ziel dieses Kapitels ist es die verschiedenen Lösungsmöglichkeiten aufzuzeigen und die unterschiedlichen Hardwareanforderungen darzustellen.

Aus Gründen der Übersichtlichkeit wurde auf die redundante Darstellung der Komponenten verzichtet.

3.2.1 Referenzarchitektur 0 - Typische DMZ

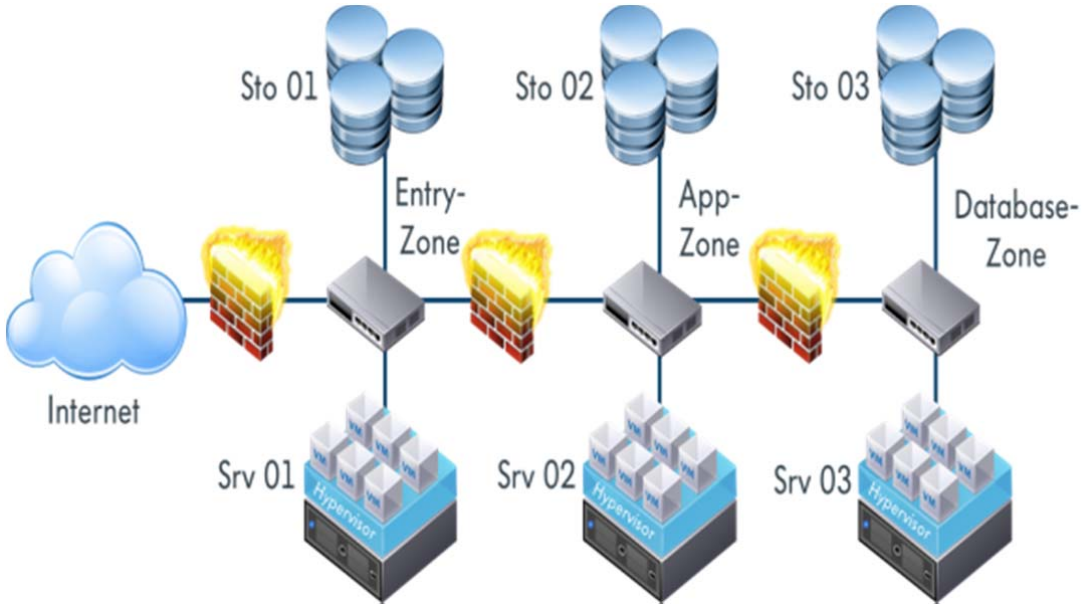

Abbildung 12: Typische DMZ

Die typische DMZ hat einen mehrstufigen Aufbau bei dem die unterschiedlichen Sicherheitszonen voneinander mittels Sicherheitsgateways (Firewalls) getrennt sind.

Die Anbindung der Speichersysteme erfolgt über dasselbe physikalische Netz, über das auch die virtuellen Maschinen (Mandanten) angebunden sind. Daraus folgt auch, dass hier technologiebedingt nur Netzwerkspeicher eingesetzt werden kann. Der Einsatz von Fibre-Channel SAN ist hier aufgrund der unterschiedlichen Protokolle nicht möglich.

Denkbar wäre auch auf die in Abbildung 12 gezeigten Speicher *Sto 01* und *Sto 02* zu verzichten und den Servern *Srv 01* bis *Srv 03* den Zugriff auf das Speichersysteme *Sto 03* über die Firewall hinweg zu ermöglichen.

Unabhängig vom gewählten Ansatz ist zumindest eine **logische** Trennung zwischen Mandantennetz und Speichernetz zwingend erforderlich. [vSHG_2013]

3.2.2 Referenzarchitektur 1 - DMZ mit separaten Backend-Switchen und Storage

Die Abbildung 13 stellt eine partiell aufgebrochene demilitarisierte Zone mit separaten physikalischen Sicherheitsbereichen dar. Organisationen die zu einer physikalischen Separierung tendieren favorisieren diesen Lösungsansatz. In dieser Konfiguration, sind die Virtualisierungshosts an separate physikalische Switche und Disksubsysteme angeschlossen.

Bei dieser Aufbauvariante halten sich die Konsolidierungsmöglichkeiten und die damit einhergehenden Effizienzvorteile in Grenzen. Durch die strickte physikalische Trennung werden aber die Auswirkungen von Fehlkonfigurationen stark eingeschränkt.

Vorteile:
- Geringe Chance von Fehlkonfiguration auf Grund geringerer Komplexität
- Höchstmaß an Sicherheit

Nachteile:
- Geringere Konsolidierung und Nutzung von Ressourcen
- Höhere Kosten durch den x-fachen Aufbau pro Sicherheitsbereich und zusätzlicher Kühl- und Stromkosten

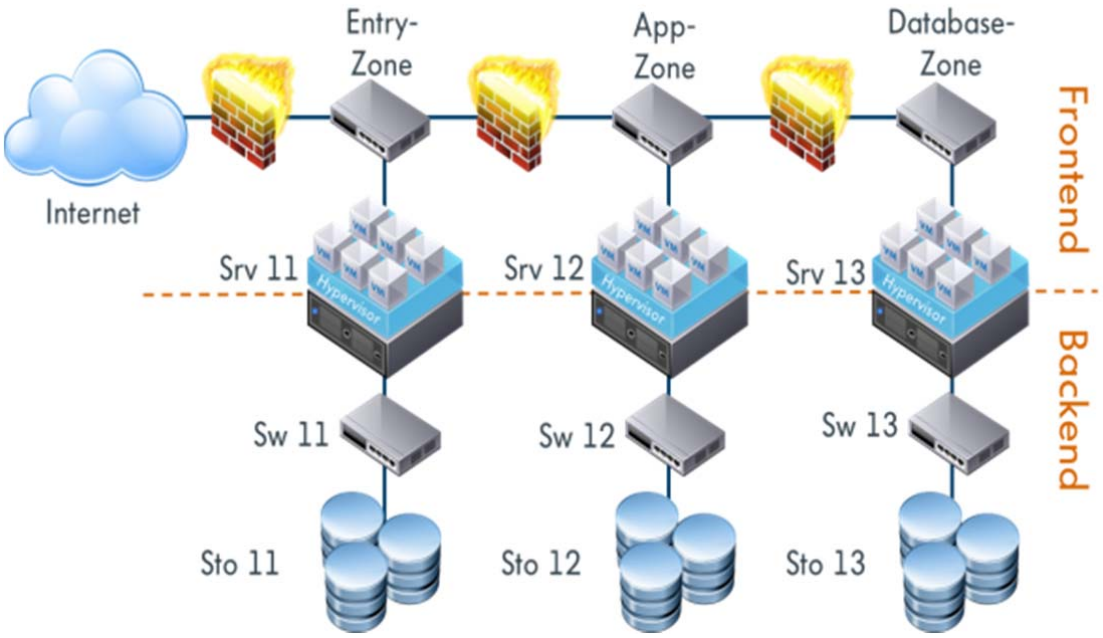

Abbildung 13: DMZ mit separaten Backend-Switchen und Storage

3.2.3 Referenzarchitektur 2 - DMZ mit separaten Backend-Switchen und zentralem Storage

Die Abbildung 14 stellt eine Konfiguration mit konsolidiertem Disksubsystem dar. Die Switch-Technik ist weiterhin in dedizierte physikalische Sicherheitsbereiche aufgeteilt. Durch die Konsolidierung des Disksubsystemes können freie Speicherressourcen, in den Sicherheitsbereichen zur Verfügung gestellt werden, in denen der Bedarf besteht. Die Auswirkungen, die durch Fehlkonfiguration im Disksubsystem entstehen können sind größer, als bei einem Aufbau mit separaten physikalischen Sicherheitsbereichen. Eine hohe Netzwerksicherheit ist durch physikalische Trennung aber immer noch gegeben.

Vorteile:
- Höhere Speichernutzung
- Geringere Kosten

Nachteile:
- Komplexerer Konfiguration
- Höhere Wahrscheinlichkeit von Fehlkonfigurationen und damit höherer Aufwand für Auditierung von Konfigurationseinstellungen.

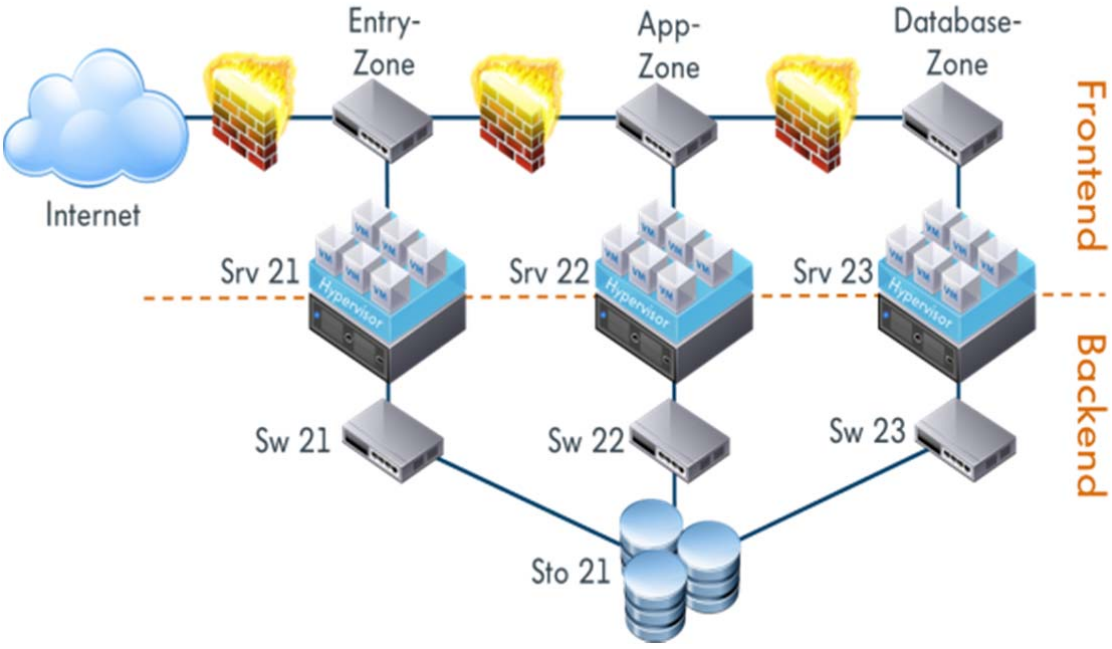

Abbildung 14: DMZ mit separaten Backend-Switchen und zentralem Storage

3.2.4 Referenzarchitektur 3 - DMZ mit zentralen Backend-Switchen und Storage

In Abbildung 15 wird der klassische SAN-Ansatz mit zentralem Backend-Switch und Storage dargestellt. Die Segmentierung erfolgt sowohl auf Netz- und Speichersystemebene und stellt das größtmögliche Maß an Konsolidierung dar. Dieser Aufbau erfordert, dass höchste Maß an Sorgfalt bei der Konfiguration, damit Rechnersysteme nur Zugriff auf die Ressourcen erhalten, die sie tatsächlich benötigen.

Vorteile:
- Größtes Maß an Konsolidierung
- Geringste Kosten

Nachteile:
- Komplexeste Konfiguration
- Größte Auswirkung bei Fehlkonfigurationen und damit höchster Aufwand für Auditierung von Konfigurationseinstellungen.

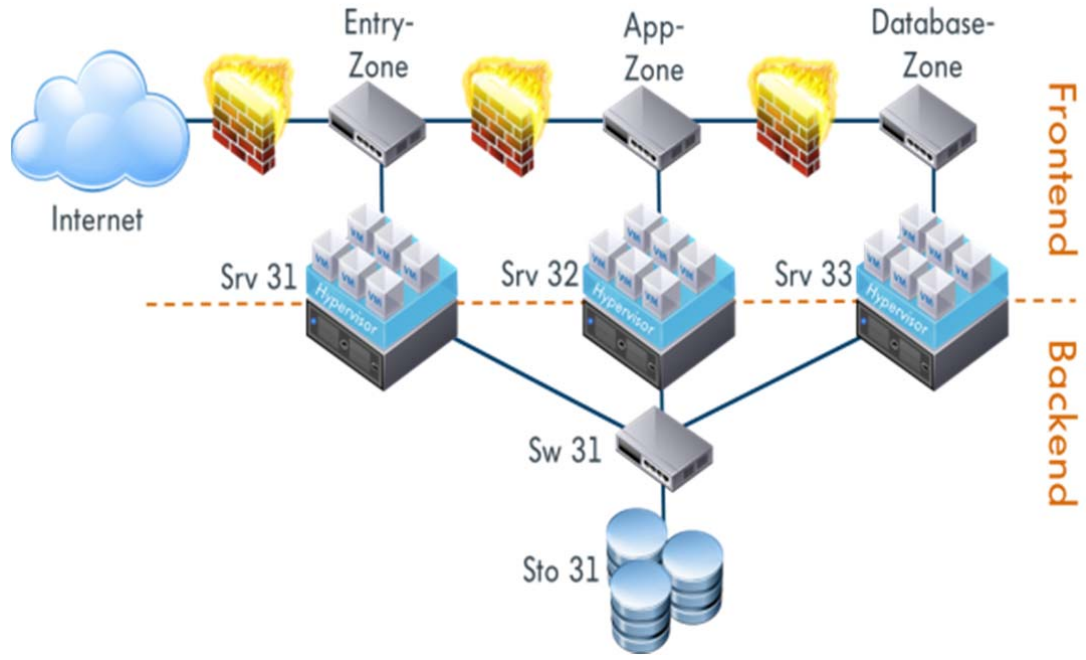

Abbildung 15: DMZ mit zentralen Backend-Switchen und Storage

4 Identifikation der Gefährdungen und Risiken und Definition der Gegenmaßnahmen

Das folgende Kapitel beschäftigt sich mit der Identifikation und Darstellung der Gefährdungen und Risiken, die bezüglich der Integration von Speichernetzen bestehen und der Definition von Gegenmaßnahmen.

Abgeleitet von den in Kapitel 1 beschriebenen Referenzarchitekturen 0 bis 3, wird im Zuge der Virtualisierung eine immer weitere Zusammenlegung von Netz und Speichersystemen ersichtlich. Hierdurch werden Systeme von unterschiedlichen Kunden bzw. Applikations-Tiers[10] auf einer gemeinsamen Hardware zusammengefasst, die logisch voneinander getrennt sind. Neben Konfigurationsfehlern, besteht die größte Gefährdung darin, wenn es erreicht wird diese logische Trennung zu umgehen.

Als Ausgangspunkt für die Risikoanalyse werden den betrachteten Zielobjekten, Server, Switche und Storage, die jeweiligen Gefährdungen zugeordnet. [BSI_1002]

Sicherheitsrisiken, die in Bezug auf SAN Umgebungen bestehen werden, oft unterschätzt. Das Fibre Channel Protokoll enthält unter Anderem diverse Schwachstellen, die auch schon aus IPv4 bekannt sind.

Die Betrachtungen dieses Kapitels sind die Grundlage zur Bewertung unterschiedlicher Speichernetzimplementierungen und orientieren sich an der ergänzenden Sicherheitsanalyse wie sie der BSI-Standard 100-2 vorsieht. Ziel ist es, eine Übersicht über die Gefährdungen zu erstellen, die auf die betrachteten Zielobjekte des Informationsverbunds wirken. [BSI_1002]

Zudem werden jeder Gefährdung Maßnahmenempfehlungen zur Absicherung des Informationsverbundes zugeordnet. Diese Maßnahmen können sowohl die Planung, Umsetzung und Betrieb von IT-Komponenten betreffen. [BSI_1002]

Dazu wird jeder Gefährdung einzeln durchlaufen und mit Maßnahmen belegt. Bei der Maßnahmenvergabe wird zwischen „Muss“ und „Kann“-Maßnahmen unterschieden. Eine „Muss“-Maßnahme muss zwingend umgesetzt werden, denn eine Nicht-Umsetzung hätte fahrlässige Auswirkungen auf das Sicherheitsniveau. Ein „Kann“-Maßnahme hingegen

[10] Ein Tier beschreibt eine Schicht in der Schichtenarchitektur wie z.B. den dreischichtigen Aufbau mit Web-, Applikations- und Datenbankservern.

wird als optional betrachtet, denn die Umsetzung hängt hierbei von der Verbesserung des Sicherheitsniveaus (Restrisikoreduzierung) und Wirtschaftlichkeit ab.

Die Maßnahmenvergabe erfolgt nach dem Maximumsprinzip. Hierbei wird der Schutzbedarf des Gesamtsystems von dem System mit dem höchsten Schutzbedarf abgeleitet. [SfIS_2014] Innerhalb eines Applikationstiers ist davon auszugehen, dass Mandanten (virtuelle Maschinen) unterschiedlichen Schutzbedarfs betrieben werden. Denkbar wären hier im Bereich der Entry-Zone.

Anwendung	**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**
Öffentlicher Webserver	Nicht relevant	Niedrig	Normal
Mail-Server	Hoch	Hoch	Hoch

Tabelle 2: Schutzbedarf unterschiedlicher Anwendungen [SuSz_2014]

Diesem Umstand wird bei der Maßnahmenvergabe entsprechend Rechnung getragen. Das BSI empfiehlt bei hohem Sicherheitsniveau die Authentisierungsinformationen und Daten verschlüsselt zu übertragen. [AeAW_2014]

4.1 Gefährdungen für das Zielobjekt „Server“

Durch den Einsatz der Server als Hypervisor[11], der virtuelle Server bereitstellt, ergeben sich auf Grund der diversen Funktionen und der Manipulationsmöglichkeiten für virtuelle IT-Systeme vielfältige Gefährdungen. Grund dafür ist die Entstehung eines neuen Infrastrukturbestandteils, die Virtualisierungsinfrastruktur für IT-Objekte. [B_Virt3304]

Die Gefährdungen innerhalb des Hypervisors sind unabhängig von der eingesetzten Speichertechnologie und sowohl bei NAS und SAN zu berücksichtigen. Dabei könnte ein Angreifer eine aktuell bestehende Verwundbarkeit im Hypervisor ausnutzen, um Zugriffsrechte zu erlangen.

Nachfolgend sind die Gefährdungen eines Hypervisor-Systems, die Auswirkungen auf gespeicherte Daten haben können, dargestellt.

4.1.1 Virtual Machine Escape

„VM Escape“ beschreibt, dass aneignen von Zugriffsrechten auf eine fremde virtuelle Maschine oder den Hypervisor selbst durch eine kompromittierte VM. [CSSE2011] Dabei nutzt der Angreifer eine bestehende Schwachstelle im Hypervisor aus und führt innerhalb einer virtuellen Maschine schadhaften Code aus um direkt mit dem Hypervisor zu intera-

[11] Ein Hypervisor ist ein Computerprogramm das virtuelle Maschinen bereitstellt. Abstrahiert ist der Hypervisor eine Schicht zwischen Hardware und virtueller Maschine.

gieren. Solch eine Schwachstelle könnte dem Angreifer Zugriff auf das Host Betriebssystem als solches und die darauf laufenden virtuellen Maschinen geben.

Virtuelle Maschinen sind so angelegt, dass sie gekapselt innerhalb der Virtualisierungsschicht ausgeführt werden (siehe Abbildung 16). Dabei sollten sie isoliert vom Host-Betriebssystem und anderen virtuellen Maschinen ausgeführt werden. Der Hypervisor arbeitet hierbei als Vermittler zwischen der VM und dem Host-Betriebssystem und verwaltet die Systemressourcen wie Prozessor und Arbeitsspeicher und teilt diese, wie benötigt, den virtuellen Gästen zu.

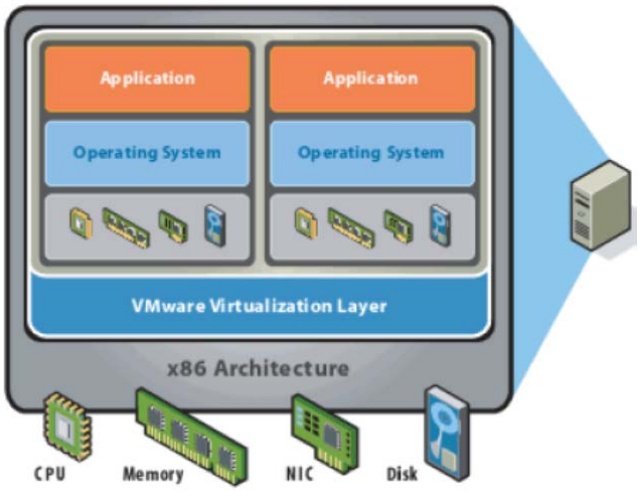

Abbildung 16: Virtualisierungsarchitektur von VMWare [AvGt_2009]

Ein gangbarer Weg, wäre das Ausnutzen von Schwachstellen in den Geräten (Devices) der VMs. Denn diese „laufen“ auf dem Host und auf diese kann vom Gast aus zugegriffen werden. [AvGt_2009]

Muss-Maßnahmen:

M 4.1.1.1 – Patch-Management des Hypervisor etablieren

Zur Beseitigung eventuell auftretender Schwachstellen im Hypervisor ist es unerlässlich ein Patch-Management für diesen einzuführen. Hierzu zählt das Bereitstellen, Verwalten und die Kontrolle der Softwareaktualisierungen, um Sicherheitslücken zu schließen. Das Patch-Management kann dabei sowohl festen Zyklen (z.B. einmal im Monat) und auch Sofortmaßnahmen (z.B. nach der Veröffentlichung kritischer Updates) folgen.
--> siehe BSI - B 1.14 Patch- und Änderungsmanagement

M 4.1.1.2 – Patch-Management der virtuellen Gäste etablieren

Zur Beseitigung eventuell auftretender Schwachstellen in den virtuellen Gästen ist es unerlässlich ein Patch-Management für diese einzuführen. Hierzu zählt das Bereitstellen, Verwalten und die Kontrolle der Softwareaktualisierungen, um Sicherheitslücken zu schließen. Das Patch-Management kann dabei sowohl festen Zyklen (z.B. einmal im Monat) und auch Sofortmaßnahmen (z.B. nach der Veröffentlichung kritischer Updates) folgen.
--> siehe BSI - B 1.14 Patch- und Änderungsmanagement

M 4.1.1.3 - Härtungsvorgaben der Hersteller befolgen

Zur Sicherung eines zuverlässigen Betriebes der Virtualisierungsinfrastruktur ist der Aufbau nach den Härtungsvorgaben des jeweiligen Softwareherstellers erforderlich. Hier wären der Hyper-V Security Guide oder der VMWare Hardening Guide zu nennen. Diese legen unter anderem fest, dass nicht benötigte Geräte und Funktionen in virtuellen Maschinen (wie z.B. CDROM-Laufwerke oder 3D-Unterstützung) zu deaktivieren sind.
--> siehe BSI - M 2.447 Sicherer Einsatz virtueller IT-Systeme

4.1.2 Überbuchung von Speicherressourcen

Wird der Speicher auf dem die virtuellen Maschinen abgelegt sind überbucht (Thin Provisioning[12]) und erzeugt eine kompromittierte VM so viel Datenaufkommen, dass der Speicherplatz erschöpft ist, dann verweigert der Virtualisierungsserver den virtuellen IT-Systemen weitere Schreibzugriffe auf die virtuellen Festplatte und die virtuellen IT-System geraten in eine Fehlersituation. Hierdurch können in den virtuellen IT-Systemen Festplattenfehler auftreten, die zu Inkonsistenzen der abgespeicherten Daten führen können. [Res_G477] [SiKo_M4346]

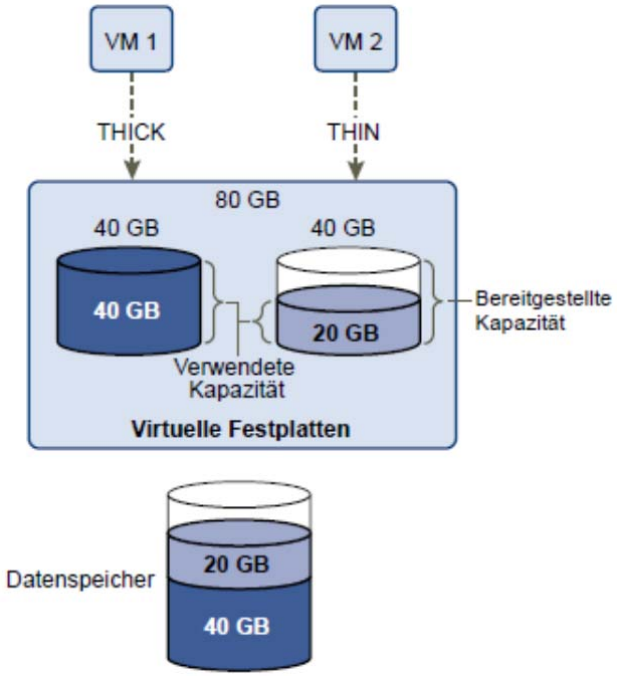

Abbildung 17: Virtuelle Festplatten [vSSp_5_1]

Der in Abbildung 17 im Thin-Format erstellten virtuellen Festplatte der VM2 wurden 40GB zugewiesen. Da aber nur 20 GB tatsächlich genutzt werden, werden auch nur 20GB auf dem Speichersystem belegt. Bei der VM1, die im Thick-Format bereitgestellt wurde, wer-

[12] Thin Provisioning ermöglicht es mehr virtuellen Speicherplatz zu vergeben, als physikalisch zur Verfügung steht.

den unabhängig vom Füllgrad der virtuellen Festplatte innerhalb der VM die gesamten 40GB auf dem Disksubsystem belegt.

Muss-Maßnahmen:

M 4.1.2.1 - Verhältnis der Überbuchung in Maßen halten

Es sollte niemals einer einzelnen virtuellen Festplatte mehr Speicherkapazität zugewiesen werden, als in der Physik zur Verfügung steht. Denn in diesem Fall könnte eine virtuelle Maschine ohne weiteres das Speichersystem überbuchen. Zudem sollte ein gesundes Maß an virtuellem zu physikalischem zugewiesenem Speicher zur Verfügung stehen, um auf ein steigendes Datenaufkommen noch zeitnah reagieren zu können.

M 4.1.2.2 - Warnungen / Alarme bei bestimmten Füllgraden setzen

Beim Einsatz von Thin-Provisioning sollte die tatsächliche Speichernutzung überwacht werden. Dies kann z.B. durch die Definition von Warnungen und Alarmen bei bestimmten Füllgraden der LUNs erfolgen. Der Speicheradministrator ist dann in der Lage, bevor die LUN überfüllt wird, diese zu vergrößern. Oder es kann durch Verteilalgorithmen (z.B. VMWare Storage vMotion) eine automatische Umverteilung von virtuellen Maschinen auf noch freie Speicherressourcen erfolgen. [vSSp_5_1]

Kann-Maßnahmen:

M 4.1.2.3 – Verzicht auf Thin Provisioning

Statt Thin-Provisioning wird Thick-Provisioning verwendet, dadurch wird der bereitgestellte Speicher beim Anlegen der virtuellen Festplatte umgehend allokiert. Eine Überbuchung ist nicht mehr möglich.

M 4.1.2.4 - Festlegung der Hardwareressourcen eines Gastes

Dem Gast wird keine virtuelle Festplatte, sondern eine dedizierte physikalische LUN zugewiesen wird (--> VMware Raw Device Mapping)

4.1.3 Fehler im Bandbreitenmanagement

Eine kompromittierte VM verursacht extremen Speicherverkehr und nutzt dadurch die physikalischen Ressourcen so sehr aus, dass andere virtuelle IT-Systeme in Mitleidenschaft gezogen werden. [Res_G477]

Muss-Maßnahmen

M 4.1.3.1 – Bandbreite begrenzen

Die Bandbreite mit der ein virtuelles IT-System auf das Speichernetz zugreift wird begrenzt. Einige Hypervisor bieten hierzu Funktionen an, die die Latenz und die Anzahl an Input/Output-Operationen pro Sekunde in „Echtzeit“ für jede LUN erfassen und bei konkurrierendem Zugriff mehrerer virtueller Maschinen den Durchsatz begrenzen. Dies kann durch Vorgabe fester Werte (Thresholds) oder durch prozentuelle Aufteilungen (Shares) erfolgen. [OpSc_2012]

4.1.4 Unautorisiertes Mitlesen oder Stören des Virtualisierungsnetzes durch unzureichende Trennung von Mandanten und internen Netzen

Personen, die unautorisiert Zugang zum Virtualisierungsnetz erlangen, können vertrauliche Inhalte der Gastsysteme mitlesen. Ein manipulierter Virtualisierungsserver kann das Virtualisierungsnetz darüber hinaus stören, in dem der Angreifer auf die im Netz übertragenen Informationen zugreift und Netzpakete unterdrückt oder verändert. [Res_G477]

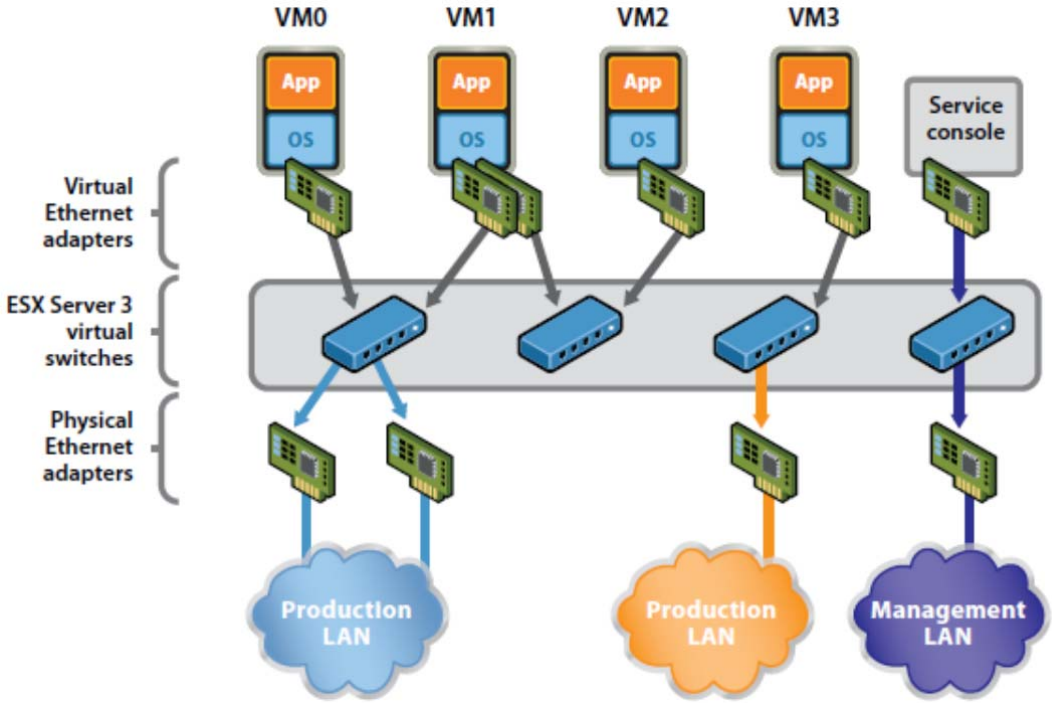

Abbildung 18: Netzwerkverbindungen virtueller Maschinen und der Service-Konsole beim VMWare ESXi [VVNC_2007]

Abbildung 18 zeigt exemplarisch den netzwerktechnischen Aufbau eines Virtualisierungshosts. Hierbei sind zwei unterschiedliche Produktionsnetze an den Virtualisierungsserver geführt worden. Das Management des Servers wird über ein dediziertes physikalisch getrenntes Netz durchgeführt.

Datenverkehr von IP-basiertem Storage, Managementanschlüssen und Datenverkehr der in Folge des Verschiebens von virtuellen Maschinen zwischen zwei Hypervisor entsteht (VMware vMotion, Microsoft Live Migration) ist von den Produktionsnetzen in denen sich die virtuellen Maschinen befinden zu trennen. [vSHG_2013]

Muss-Maßnahmen

M 4.1.4.1 - Virtuelle Trennung der Netzsegmente

Eine Möglichkeit die unterschiedlichen Datenverkehrsarten zu trennen ist die logische Trennung. Ein bewährtes Mittel hierbei ist die Verwendung von VLANs (virtuellen Netzen).

M 4.1.4.2 - Ungeeignete Konfiguration der aktiven Netzkomponenten vermeiden

Ungeeignete Konfiguration kann vermieden werden, in dem nicht benötigte, aber konfigurierte VLANs die auf Netzwerkanschlüsse gelegt wurden, entfernt werden. [CSSE2011] Zudem sollten alle Einstellungen dokumentiert und die Konfiguration überwacht und geprüft sein. [vSHG_2013]

Kann-Maßnahmen

M 4.1.4.3 - Physische Trennung der Netzsegmente

Sollte eine virtuelle Trennung mittels VLANs nicht ausreichend sein, besteht die Möglichkeit die unterschiedlichen Netze physikalisch voneinander zu trennen. Denkbar wäre z.B. eine physikalische Trennung nach Produktionsnetz, Managementnetz und Migrations- und Speichernetz.

4.2 Gefährdungen für das Zielobjekt „Ethernet-Switch“

In diesem Kapitel werden Gefährdungen beschrieben, die den Ethernet-Switch / Router betreffen.

Die Gefährdungen die hierbei bestehen basieren auf bekannten Schwachstellen der eingesetzten Protokolle, wie MAC, TCP und STP. [RuS_B3302]

Nachfolgend sind die Gefährdungen eines Switches / Routers beim Einsatz in Speichernetzen dargestellt:

Zu unterscheiden sind hierbei:

Remote Attacken, bei denen ein Angreifer versucht von dem System, an dem er aktuell angemeldet ist, auf ein anderes System über das Netz zuzugreifen. Zum Bespiel könnte das Ziel hierbei sein, über eine Man-In-The-Middle-Attacke, den Netzwerkverkehr von einem anderen System abzufangen und aufzuzeichnen.

Und *Denial-of-Service-Attacken* bei denen ein Dienst der eigentlich verfügbar sein sollte, nicht verfügbar ist. Die Gründe hierfür können vielfältig sein, sind aber in der Regel die Folge einer Überlastung in der IT-Infrastruktur. Dies kann unbeabsichtigte Überlastungen oder einen mutwilligen Angriff als Ursache haben.

4.2.1 MAC Flooding

Ein Ethernet-Switch speichert in seiner Source Address Table (SAT) die MAC-Adressen der an ihn angeschlossenen Geräte. Dadurch wird der Switch in die Lage versetzt die Ethernet-Pakete zielgerichtet an die Empfänger weiterzuleiten. [MacF_2013]

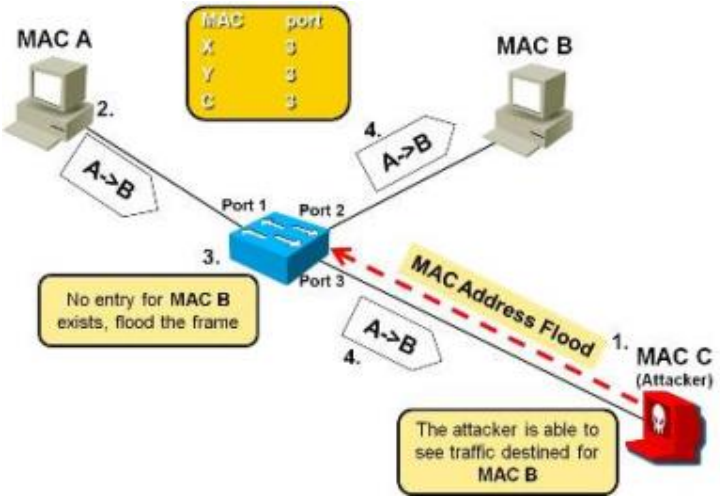

Abbildung 19: MAC-Flooding [SHAS_2012]

Beim MAC-Flooding versucht ein Angreifer die Netz-Switche durch das Senden von vielen Ethernet Frames mit wechselnden Quell-MAC-Adressen zu "überfluten" (1). Der Netz-Switch würde, sobald das Limit seiner MAC-Adressen erreicht ist, eingehende Verbindungen, bislang bekannter MAC-Adressen (2), nicht mehr mittels seiner Address Table zuordnen können (3) und die Daten als Broadcast[13] versenden. Der Switch arbeitet jetzt als Hub. Der Angreifer kann dadurch den Netzverkehr fremder Teilnehmer sehen (4). Virtuelle Switche sind hiervon nicht betroffen, da sie keine MAC-Adressen „lernen“. [CSSE2011]

Muss-Maßnahmen

M 4.2.1.1 – Einsatz von Port Security auf Netzwerkswitchen

Port Security ist eine Funktion von Netzwerkswitche bei dem jedem Port eine oder mehrere feste MAC-Adressen zuordnet werden. Der Switch prüft hierzu bei jedem Verbindungsaufbau die Absenderadresse, bevor Nutzdaten übertragen werden. Hat sich die Absenderadresse geändert, setzt der Switch den Port auf den Status „Down“, bis er nicht wieder administrativ auf „Up“ gesetzt wird. [PoSe_2013]

Kann-Maßnahmen

M 4.2.1.2 – Verwendung von dynamischen VLANs

Dynamische VLANs können durch den Einsatz von Softwarelösungen implementiert werden. Hierzu wird eine VLAN Configuration Server installiert. Bei der Verwendung von dynamischen VLANs findet einer Zuordnung von MAC-Adressen zu VLANs statt. Sobald ein

[13] Bei einem Broadcast werden Daten von einem Punkt aus an alle Teilnehmer eines Nachrichtennetzes übertragen. [Broc_2014]

Gerät dem Netzwerk beitreten möchte, gleicht der Switch die MAC-Adresse des Gerätes mit dem Configuration Server ab und ordnet das entsprechende VLAN dynamisch zu. So wird der Zugriff auf eine VLAN nur MAC-Adressen ermöglicht, die auch für dieses VLAN freigeschaltet sind. [EiVL_2006]

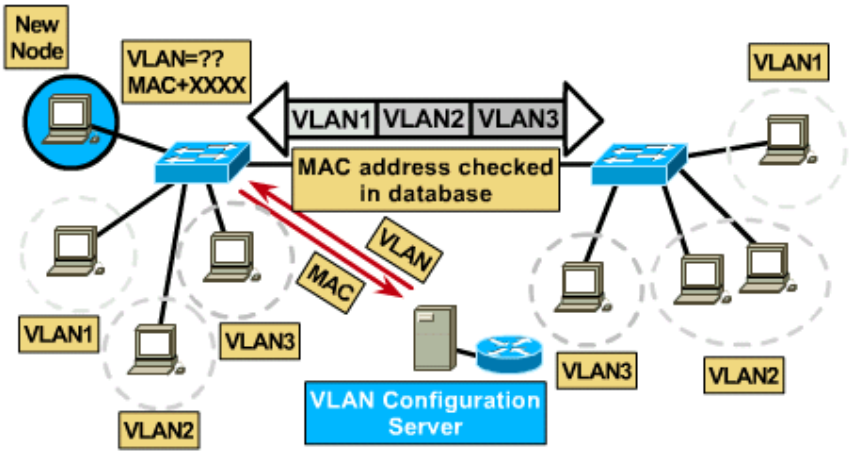

Abbildung 20: Aufbau von dynamischen VLANs[VLan_2013]

M 4.2.1.3 – Verwendung von IEEE 802.1X zur Authentifizierung

IEEE 802.1x beschreibt ein sicheres Authentifizierungsverfahren für die Zugangskontrolle in lokalen Netzen. Einhergehend mit IEEE 802.1x wird oft RADIUS[14] zur Authentifikation genannt.

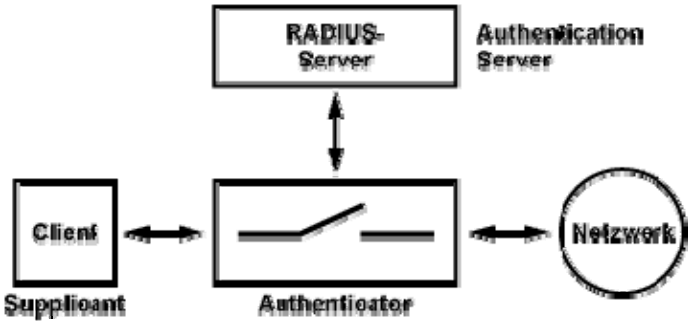

Abbildung 21: Funktionales Blockschaltbild IEEE802.1x [IERa_2014]

Bestandteile des IEEE802.1x Authentifizierungsverfahrens sind die in Abbildung 21 dargestellten Komponenten. Hierzu zählen der Supplicant (Antragsteller), der Authenticator (Beglaubigter) und der Authentication Server (z.B. ein RADIUS-Server), der die Anfrage des Supplicant überpüft und seine Entscheidung dem Authenticator mitteilt, dieser schaltet dann entweder den Zugang zum Netz frei oder verweigert ihn.

[14] RADIUS ist ein Client-Server-Protokoll, das zur Authentifizierung und Autorisierung von Benutzern bei Einwahlverbindungen in ein Computernetzwerk dient. [IE802x_2014]

Folgende Zuordnungen können hierbei getroffen werden:

- Supplicant (Antragsteller): Ein LAN-Port / eine LAN-Station
- Authenticator (Beglaubigter/Unterhändler): ein Switch mit IEEE802.1x
- Authentication Server : RADIUS-Server

Sollte die LAN-Station keine IEEE-802.1x-Authentisierung im Netzwerk unterstützen, gibt es die Alternative, die Geräte mittels ihrer MAC-Adresse am Switch zu authentisieren. Hierzu nimmt der Switch die MAC-Adresse des Hosts als Benutzernamen und Passwort. [IERa_2014]

M 4.2.1.4 – Statische Einträge in MAC-Adresstabelle
Für kritische Systeme können statische Einträge in der MAC-Adresstabelle vorgenommen werden. Diese sind dann vom MAC-Flooding ausgenommen. [LANS_2004]

4.2.2 MAC Spoofing

Bei diesem Angriff verwendet ein Angreifer eine gefälschte MAC-Adresse um Sicherungsmechanismen zu umgehen (Port Security oder dynamische VLANs) oder um die Identität eines Opfers vorzugeben und dessen Netzverkehr an sich zu ziehen.

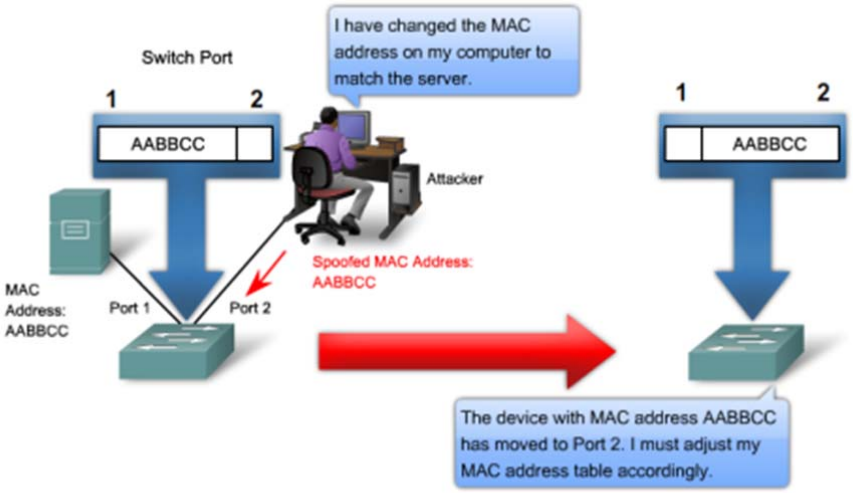

Abbildung 22: MAC Spoofing [L2AM_2012]

Netzswitche lernen die Zuordnung der MAC-Adresse zum Port über die Quell-MAC-Adressen des empfangenen Datenverkehrs. Wenn ein Angreifer eine gefälschte MAC-Adresse verwendet, so ändert der Switch diese Zuordnung und sendet den Verkehr anstatt zum Opfer zum Angreifer. Nach dem die Zuordnung geändert wurde, werden dem Opfer vom Switch keine Pakete mehr zugestellt. [CSSE2011]

Sendet das Opfer nun wieder Daten an den Switch, passt dieser die MAC-Adresse-zu-Port-Zuordnung wieder auf den ursprünglichen Wert an. [L2AM_2012]

Damit dieser Angriff funktioniert, muss sich der Angreifer im selben Netz befinden wie das Opfer. [CSSE2011]

Muss-Maßnahmen

M 4.2.2.1 – Einsatz von Port Security auf Netzwerkswitchen

siehe M 4.2.1.1

Kann-Maßnahmen

M 4.2.2.2 – Verwendung von IEEE 802.1X Authentifizierung

siehe M 4.2.1.3

M 4.2.2.3 – Statische Einträge in MAC-Adresstabelle

siehe M 4.2.1.4

4.2.3 Spanning Tree Angriffe

Bei diesem Angriff versendet der Angreifer sogenannte BPDUs (Bridge Protocol Data Units) mit dem Ziel, die Netzswitche dazu zu bringen, den Angreifer als Root Bridge (rogue root bridge) anzusehen. Im besten Fall für den Angreifer könnte der Netzverkehr dann über seine Maschine übertragen werden, sodass er als Man-in-the-Middle (MITM) den Netzverkehr mitschneiden könnte. Gelingt es einem Angreifer sich als MITM zu etablieren, dann könnte er dieses aber auch dazu nutzen DoS-Attacken zu fahren und durch falsche BPDUs das Netz dazu zwingen die Spanning-Tree Topologie neu aufzubauen, was zu Netzausfällen führt. Virtuelle Switche verwenden das Spanning-Tree Protokoll selbst nicht, leiten BPDUs aber weiter. [CSSE2011]

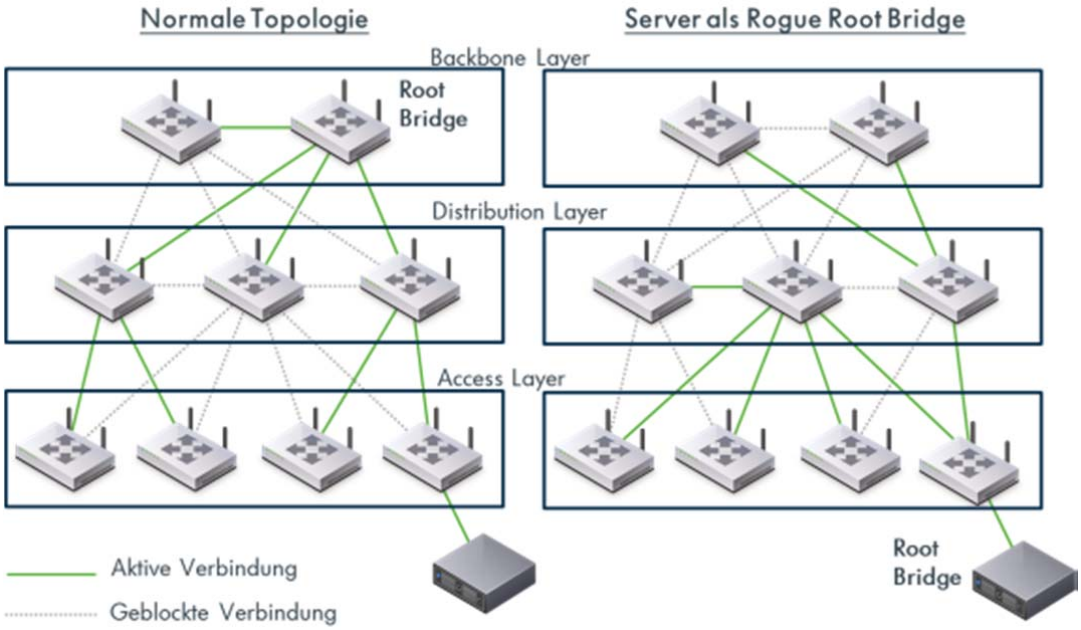

Abbildung 23: Hierarchische Netztopologie vor und nach SPT-Angriff

Muss-Maßnahmen

M 4.2.3.1 – Konfiguration von Root und BPDU Guard [CSSE2011]
Root und BPDU Guard sind Funktionsbezeichnung von Switchen der Fa. Cisco. BPDU Guard wird auf den Access-Switchen konfiguriert. Sendet ein Server BPDU-Frames ins Netz, wird dies vom Switch erkannt und der betreffende Port vom Access-Switch deaktiviert.

M 4.2.3.2 - Die Root Bridge manuell festlegen [NW_2007]
Spanning Tree sollte nicht die Möglichkeit gegeben werden die Root Bridge selbst zu bestimmen. Der Netzwerkplaner sollte die Root Bridge selbst festlegen und mit einer Priorität von 1 versehen. Somit wird vermieden, dass Geräte die sich als Switch ausgeben und BDPUs mit einer geringeren Priorität, als die der ausgehandelten Root-Bridge verschicken, zur Root-Bridge werden.

4.2.4 IP Session Hijacking

Beim IP Session Hijacking wird die bestehende Sitzung zwischen zwei Teilnehmern eines IP-Netzwerkes von einer nicht vertrauenswürdigen dritten Partei übernommen in dem die Initial Sequence Number eines IP Frames erraten und für einen Angriff verwendet wird. [Sec2005]

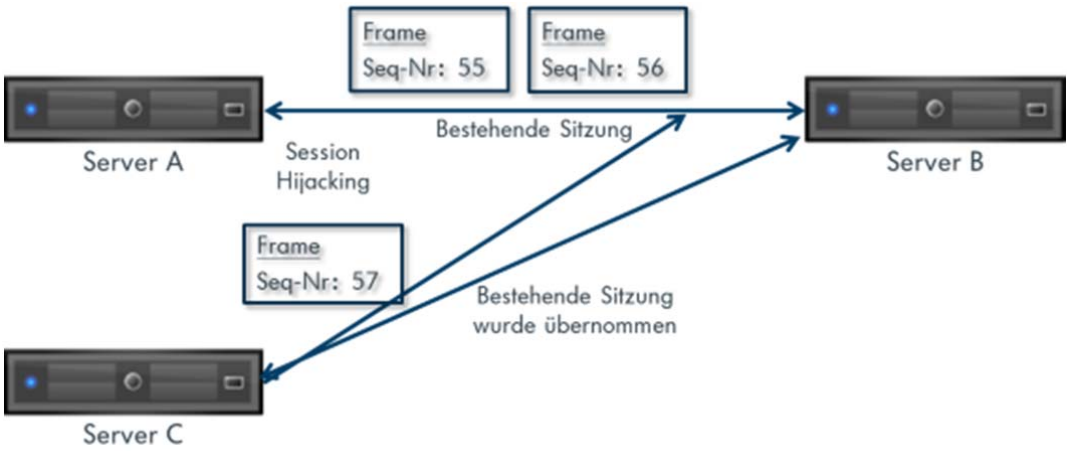

Abbildung 24: Angriffsszenario des IP Session Hijacking

Abbildung 24 skizziert das Angriffsszenario des IP Session Hijacking. Server A und Server B tauschen Pakete über eine bestehende Verbindung untereinander aus. Server C liest den Datenverkehr zwischen den beiden Geräten mit und identifiziert den Wert der Sequenznummer. Dann injiziert Server C ein Frame mit einer um eins erhöhten Sequenznummer. Server B erhält das gefälschte Frame von Server C und da es die korrekte Sequenznummer aufweist, wird es als nächstes Frame in der Sitzung erkannt. Die Sitzung wird dahin übergeben, wo sie als letztes geendet hat und zwar an die Adresse, die das falsche Frame gesendet hat. Server C hat nun die Sitzung übernommen ohne sich authentifizieren zu müssen. Server B geht weiterhin von einer bestehenden Sitzung mit Server A aus. [Sec2005]

Muss-Maßnahmen

M 4.2.4.1 - Nutzung von IPsec [BpfSN2007]

IPsec ist eine Sicherheitsarchitektur für IP, die das Internet Protokoll um Mechanismen zur Verschlüsselung und Authentisierung erweitert. [IPSecE2014] Durch diese Erweiterungen soll eine sichere Kommunikation über potentiell unsichere Netze gewährleistet werden.

IPsec wiederum besteht aus zwei weiteren Protokollen:

- Encapsulated Security Payload (ESP) verschlüsselt IP-Pakete um diese vor Manipulationen Dritter zu schützen.
- Der Authentication Header (AH) enthält eine Prüfsumme, die sicherstellt, dass ein IP-Paket nicht verändert wurde. Der Authentication-Header folgt nach dem normalen IP-Header und erlaubt dem Empfänger eines IP-Paketes, dessen Integrität zu prüfen. [VPNs_2014]. Das IP Session Hijacking würde somit ausgeschlossen werden.

4.2.5 Double-Encapsulated 802.1Q / Nested VLAN Attack

Bei diesem Angriff sendet der Angreifer Datenpakete, die in zwei VLAN Header gekapselt sind. Der erste Switch, der dieses Paket erhält entfernt den ersten VLAN Header und leitet das Paket inklusive dem zweiten VLAN Header weiter. Verwendet der Angreifer im ersten Header ein natives VLAN, dass auf dem Trunk zwischen den beiden Switchen vorhanden ist, wird dieses vom zweiten Switch akzeptiert, der VLAN Header entfernt und das Paket an die richtige MAC Adresse weitergeleitet. Eine Rückantwort ist bei diesem Angriff nicht möglich. Es besteht aber das Risiko einer DoS-Attacke. [Sec2005]

Abbildung 25: Nested VLAN Attacke [CSSE2011]

Muss-Maßnahmen

M 4.2.5.1 – Entfernen des nativen VLANs von allen Access-Ports [VSWP_2014]

Abbildung 26: Zuordnung des Access VLAN

Das native VLAN wird auf allen Access-Ports entfernt (VLAN1) und es werden nur noch die auf den virtuellen Switchen konfigurierten VLANs an den Server gelegt. [CSSE2011]

M 4.2.5.2 - Festlegen eines ungenutzten VLANs als natives VLAN für alle Trunks. [VSWP_2014]

Abbildung 27: Zuordnung des Trunk VLAN

Das native VLAN (im Auslieferungszustand eines Switches das VLAN 1) wird auf allen Trunkverbindungen auf ein nicht benutztes VLAN umgestellt (n). [CSSE2011]

4.2.6 ARP Spoofing

Das Address Resolution Protocol ist bereits eine alte Technologie. Der ARP RFC stammt aus einer Zeit in der noch jeder Netzteilnehmer tendenziell als „Freund“ angesehen wurde und aus diesem Grund fanden auch keine sicherheitstechnischen Implementierungen den Einzug in das Protokoll. Daraus resultiert, dass sich jeder als der Besitzer einer beliebigen IP-Adresse ausgeben kann bzw. es ist jedem Netzteilnehmer möglich ARP Nachrichten, innerhalb seines Subnutzes, mit einer Zuordnung seiner MAC-Adresse zu einer beliebigen IP-Adresse zu versenden. [VSWP_2014]

```
Ethernet II, Src: 00:d0:59:05:95:09, Dst: 00:04:c1:7d:d6:54
Address Resolution Protocol (reply)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (0x0002)
    Sender MAC address: 00:d0:59:05:95:09 (00:d0:59:05:95:09)
    Sender IP address: 10.185.208.154 (10.185.208.154)
    Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
    Target IP address: 0.0.0.0 (0.0.0.0)
```

Abbildung 28: Inhalt eines ARP Reply [LANS_2004]

Dies ist möglich da es keine Verifikationsmechanismen der Korrektheit von MAC-Adressen zu IP-Adressen-Zuordnung in ARP gibt. [VSWP_2014]

Die Gefährdung besteht darin, dass es einem Angreifer mit Hilfe gefälschter ARP Pakete möglich ist, die ARP Tabellen (z.B. auf Switches oder Hosts) so zu verändern, dass die MAC-Adresse des Angreifers einer fremden IP-Adresse zugeordnet wird. Hierdurch ist es dem Angreifer möglich sich als Man-In-The-Middle zu etablieren. [Sec2005]

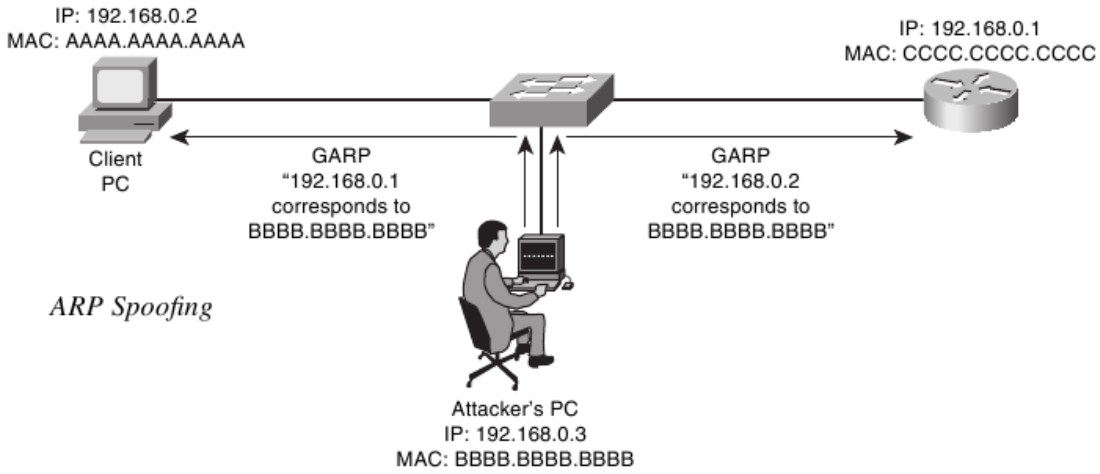

Abbildung 29: ARP Spoofing Attacke [ARP_2010]

Muss-Maßnahmen

M 4.2.6.1 – Einsatz von Port Security auf Netzwerkswitchen

Der Einsatz von Port Security kann Abhilfe schaffen, falls der Angreifer falsche MAC-Adressen benutzt. [LANS_2004]

siehe M 4.2.1.1

M 4.2.6.2 – Einsatz von DHCP Snooping

Unter den Begriff des DHCP Snoopings fällt eine Serie von Techniken, die dazu verwendet werden den sicheren Betrieb einer DHCP Infrastruktur zu gewährleisten. Hierzu werden Informationen des / der DHCP Snooping Binding Datenbank genutzt, um folgendes sicherzustellen:

- Nachverfolgung der physikalischen Standorte der Hosts
- Sicherstellung, dass Hosts nur IP-Adressen nutzen die Ihnen zugewiesen wurden
- Sicherstellung, dass nur autorisierte DHCP Server erreichbar sind [DHCPSn12]

Die Funktion des DHCP Snoopings wirkt dabei wie eine Firewall zwischen nicht vertrauenswürdigen Netzteilnehmern und den vertrauenswürdigen DHCP Servern. Dabei werden folgenden Aktivitäten durchgeführt:

- Validierung von empfangenen DHCP Nachrichten von nicht vertrauenswürdigen Quellen und herausfiltern ungültiger Nachrichten
- Begrenzung des DHCP Datenverkehrs von vertrauenswürdigen und nicht-vertrauenswürdigenden Quellen
- Aufbau und Verwaltung der DHCP Snooping Binding Datenbank, die Informationen über die nicht-vertrauenswürdigenden Netzteilnehmer und deren zugewiesene IP-Adressen und MAC-Adressen enthält.

M 4.2.6.3 – VLAN

Der Einsatz von VLANs und der damit verbunden logischen Segmentierung verringert die Größe der Broadcast-Domänen. Da die ARP Spoofing Attacke nur im jeweiligen Subnetz wirkt, kann so die Fehlerdomäne stark eingegrenzt werden. [BpfSN2007]

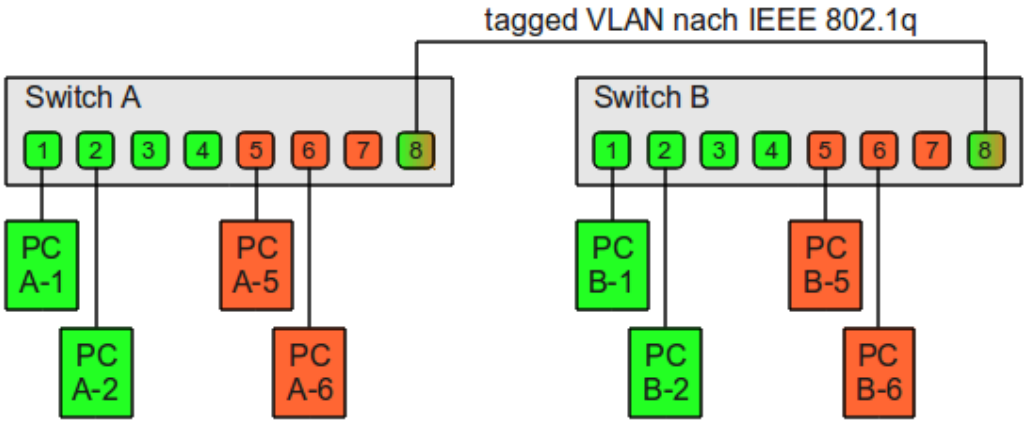

Abbildung 30: Verbindung der zwei VLANs der beiden physischen Switche [VL_G_2014]

Kann-Maßnahmen

M 4.2.6.4 – Statische ARP-Einträge

Statische ARP-Einträge für Router/Firewall und kritische Server auf den Hosts-Systemen verhindern die Veränderung. [LANS_2004]

M 4.2.6.5 – Unterbinden von Host-zu-Host Kommunikation

Durch die Bildung von privaten VLANs kann die Host-zu-Host Kommunikation auf Layer 2 Ebene unterbunden werden. Dadurch verringern sich die Broadcastdomänen entsprechend weiter. [LANS_2004]

4.3 Gefährdungen für das Zielobjekt „FC-Switch“

In diesem Kapitel werden Gefährdungen beschrieben, die den Fibre-Channel-Switch betreffen.

Die Gefährdungen die hierbei bestehen basieren auf bekannten Schwachstellen des Fibre Channel Protokolls. [RuS_B3302]

Die für die Ethernet-Switche beschriebenen Gefährdungen wie *Remote Attacken* und Denial-of-Service-Attacken sind bei FC-Switchen genau so präsent.

4.3.1 FC Session Hijacking

Beim FC Session Hijacking wird die bestehende Sitzung zwischen zwei Teilnehmern von einer nicht vertrauenswürdigen dritten Partei übernommen, in dem die Sequence Control Number und Sequence Identifcation Number eines FC Frames erraten und für einen Angriff verwendet werden. [CSSE2011]

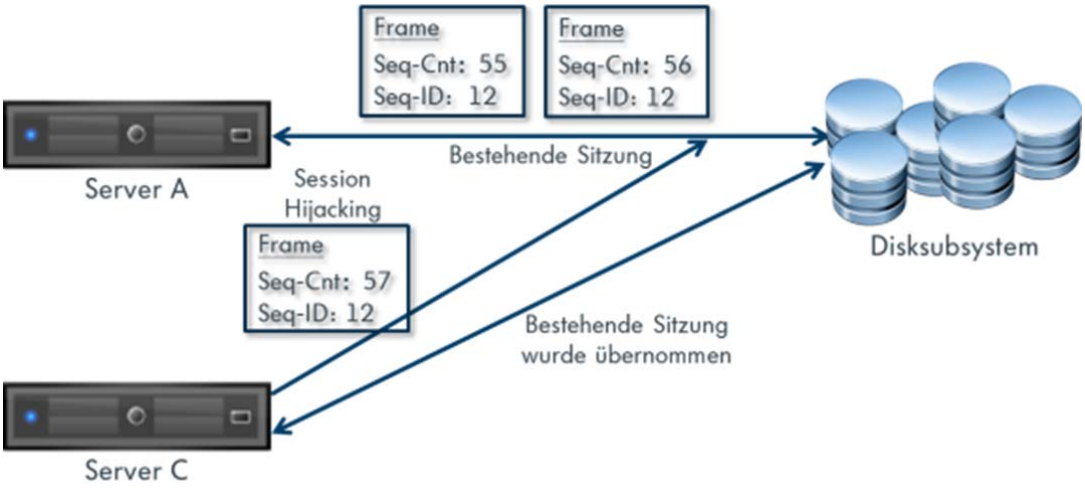

Abbildung 31: FC Session Hijacking

Abbildung 31 skizziert das Angriffsszenario des FC Session Hijacking. Server A und das Disksubsystem tauschen Pakete über eine bestehende Verbindung untereinander aus. Server C liest den Datenverkehr zwischen den beiden Geräten mit und identifiziert den Wert der Sequence Control Number und Sequence Identifcation Number. Dann injiziert Server C ein Frame mit einer um eins erhöhten Sequence Control Number und derselben Sequence ID, welches als nächstes Frame erkannt wird. Das Disksubsystem erhält das gefälschte Frame von Server C und da es die korrekte Sequenznummer aufweist, wird es als nächstes Frame in der Sitzung erkannt. Die Sitzung wird dahin übergeben, wo sie als letztes geendet hat und zwar an die Adresse, die das falsche Frame gesendet hat. Server C hat nun die Sitzung übernommen ohne sich authentifizieren zu müssen. Das Disksubsystem geht weiterhin von einer bestehenden Sitzung mit Server A aus. [Sec2005]

Muss-Maßnahmen

M 4.3.1.1 – Nutzung von FCsec

Um die gesicherte Übertragung jeder einzelnen Nachricht bzw. jedes einzelnen Frames zu gewährleisten haben die führenden Storagehersteller (Cisco, EMC, QLogic…) einen Vorschlag erarbeitet, der die Erweiterung des Fibre Channel Schicht 2 Frame-Formates, um eine Frame-zu-Frame-Verschlüsselung vorsieht. Dieses neue Frame-Format wurde in Anlehnung an das IPsec Encapsulating Security Payload, ESP Header genannt. Aufgrund der starken Ähnlichkeit zu IPsec wird dieser Sicherheitsaspekt für Fibre Channel häufig auch FCsec genannt.

Die Vorteile der FCsec Architektur liegen darin, dass sie ein Rahmenwerk zum Schutz gegen Attacken unter folgenden Sicherheitsaspekten bieten:

- Authentifikation der Datenherkunft, um sicherzustellen, dass der Absender jedes Frames authentisch ist
- Sicherstellung das Datenintegrität
- Optionale Datenverschlüsselung [ISMH_2004]

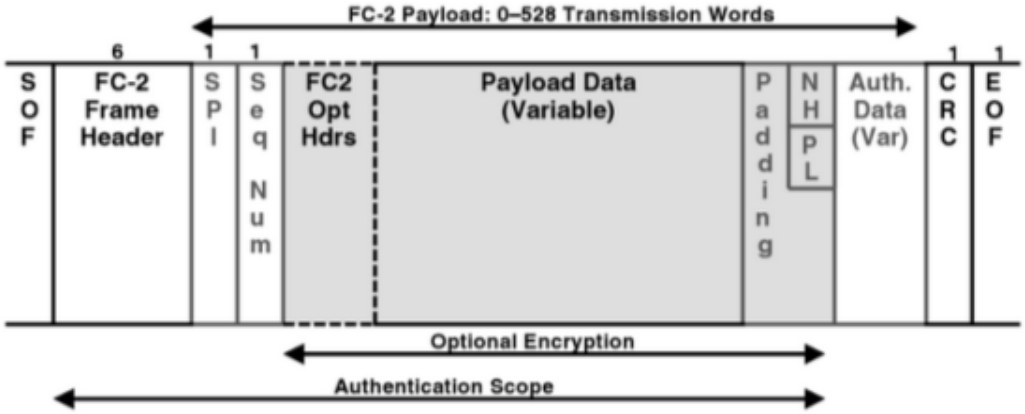

Abbildung 32: Fibre Channel Security Protocol Frame [ISMH_2004] S. 82

4.3.2 Name Server Pollution

Die Unsicherheit besteht darin, dass ein Angreifer ein gefälschtes PLOGI Frame zum Name Server sendet und dieser daraufhin ein Update seiner Datenbank mit inkorrekten Daten durchführt. Der Angreifer tauscht dabei seine tatsächliche Fabric Adresse gegen die seines zu übernehmenden Zieles aus, sodass der Datenverkehr zukünftig über ihn geleitet wird, da die Zuordnung der Fabric Adresse zur WNN nicht mehr korrekt ist. [Sec2005]

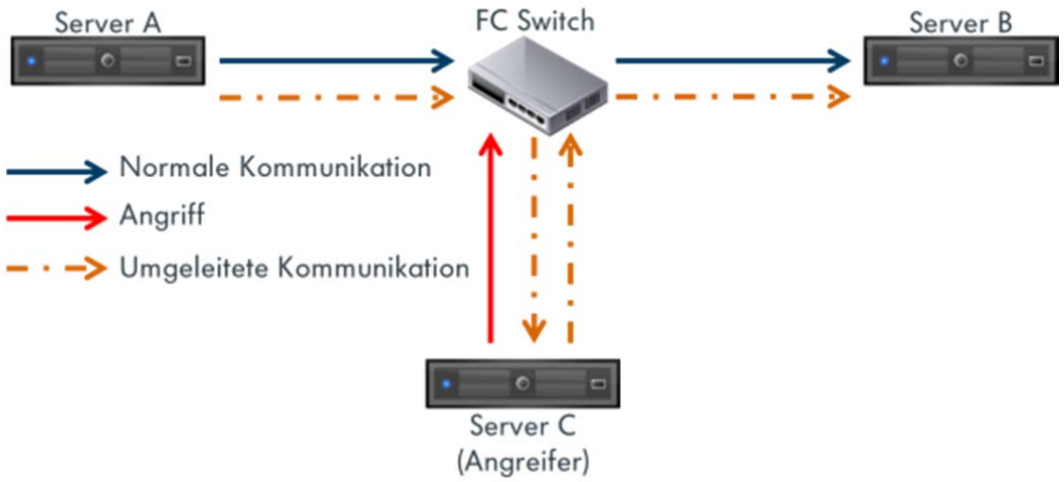

Abbildung 33: Name Server Pollution Angriff

Abbildung 33 zeigt die Name Server Pollution Attacke. Server A und Server B kommunizieren miteinander. Der Angreifer sendet kontinuierlich gefälschte PLOGI Frames an die Adresse xFFFFFC des Name Servers. Dabei versucht er den Eintrag der Namensdatenbank, für die 24-Bit-Fabric Adresse des Server B, durch seiner eigene WWN zu ersetzen. Nach dem die Änderung des Eintrages gelungen ist, wird der gesamte Datenverkehr, der für Server B bestimmt ist, an Server C gesendet. Server C kann nun den Datenstrom mitlesen und als Man-in-the-Middle fungieren. [Sec2005]

Muss-Maßnahmen

M 4.3.2.1 – Nutzung von Authentifizierungsmechanismen am Name Server

Zur Vermeidung der Name Server Pollution Attacke ist es notwendig, dass die Kommunikationsteilnehmer ihre Identität bidirektional prüfen und feststellen. Im FC-SAN sind hierfür drei Authentifizierungsmethoden vorhanden. [SFCN_2014]

- Diffie Hellman Challenge Handshake Authentication Protocol (DH-CHAP)

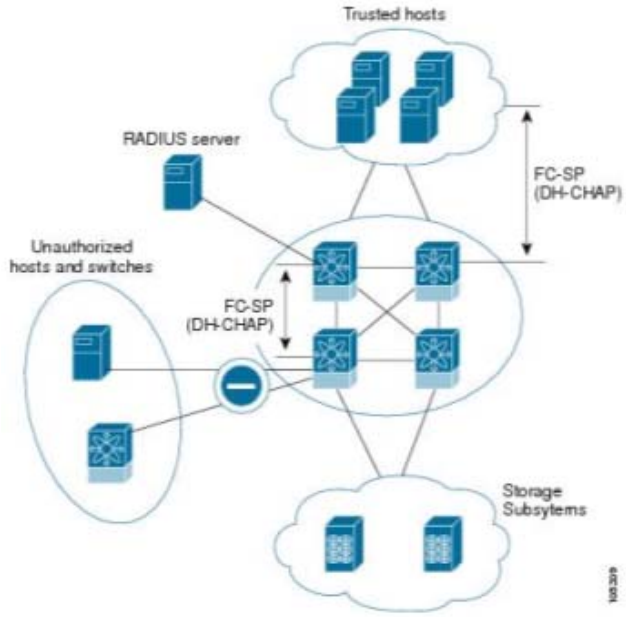

Abbildung 34: Switch und Host Authentifikation mit DH-CHAP [DHCh_2014]

DH-CHAP bietet eine bidirektionale passwort-basierende Authentifizierung, auf Basis des Challenge Handshake Authentication Protokolls, erweitert um einen Diffie-Hellmann Schlüsselaustausch. Abbildung 34 zeigt den exemplarischen Aufbau im FC SAN. [FCDH_2003] Der Radius Server fungiert hierbei als zentraler Authentifikationsserver und entscheidet, ob eine Gerät als vertrauenswürdig angesehen werden kann, also Zugriff zur Fabric erhält.

- Fibre Channel Authentication Protocol (FCAP)
In einer zertifikatsbasierenden Infrastruktur werden die einzelnen Teilnehmer der Umgebung über eine vertrauenswürdige zentrale Authentisierungsstelle zertifiziert. Zertifizierte Teilnehmer können sich dabei gegenseitig über das Fibre Channel Authentication Protocol authentifizieren. [FCSp_2004]

- Fibre Channel Password Authentication Protocol (FCPAP)
Das Fibre Channel Password Authentication Protocol ist ein auf Passwörtern basierendes Authentifikations- und Schlüsselaustauschprotokoll, welches zur gegenseitigen Authentifizierung zweier Fibre Channel Ports in einer Fibre Channel Fabric genutzt werden kann. [FCPap_2002]

M 4.3.2.2 – Verwendung von vSAN

Durch die Verwendung von virtuellen SANs können die Fehlerdomänen verringert werden. Name Server Pollution ist hierbei nur noch in den vSANs möglich auf die der Angreifer auf Grund seiner WWN oder seines Fibre-Channel-Port-Anschluss Zugriff hat. vSAN sollte verwendet werden, um unterschiedliche Applikationstiers voneinander zu trennen (Web-, Applikations- und Datenbankserver). [FCAn_2006]

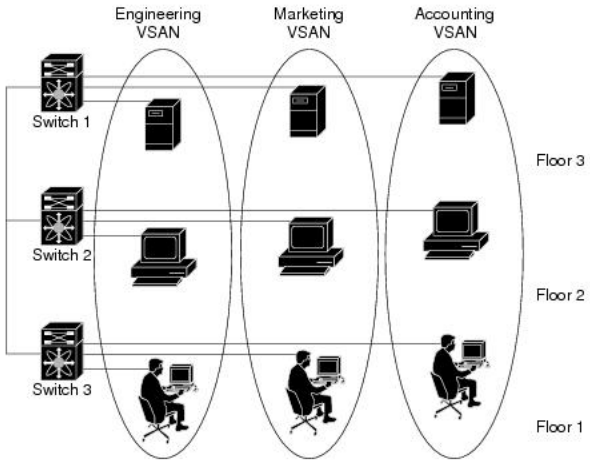

Abbildung 35: vSAN [vSAN_2014]

4.3.3 Reconfigure Fabric Attacke

Hierbei sendet der Angreifer gefälschte Änderungsbenachrichtigungen an die Fibre Channel Switche mit der Absicht den Netzwerkverkehr zu stören. [CSSE2011] Einer der Verbindungsdienste (Link Services), der von einer Fibre Channel Fabric angeboten wird, sind die RSCNs (Registered State Change Notifications). Wenn ein Event in der Fabric eintritt, wird dies allen betroffenen Ports kommuniziert. Die Nutzdaten der RSCNs könnten unter Umständen eine Liste der betroffenen N-Ports und Kommandocodes enthalten. Jeder Empfänger dieser RSCN-Nachrichten wird, abhängig vom Hersteller, mit der Durchführung von Aktionen reagieren, die Sicherstellen das die Fabric Informationen, die der jeweilige Port über die Fabric hat, korrekt sind. Dies können gewöhnlich das Ausführen von „Rediscover-Methoden“ oder Name-Server-Abfragen sein. Gewöhnlich stellt dies kein Problem dar, denn das Eintreten dieser Events reicht nicht aus um den Datenfluss zu stören. Wenn die Frequenz des Eintretens dieser Benachrichtigungen aber erhöht wird, kann es zu Störungen bzw. Abbrüchen im Datenfluss kommen. [FCAn_2006]

Muss-Maßnahmen

M 4.3.3.1 – Einsatz von Zoning

siehe Grundlagenkapitel 3.1.1.6 (Segmentierung / Zugriffsteuerung)
Durch den Einsatz von Zoning wird die Fehlerdomäne eingegrenzt.

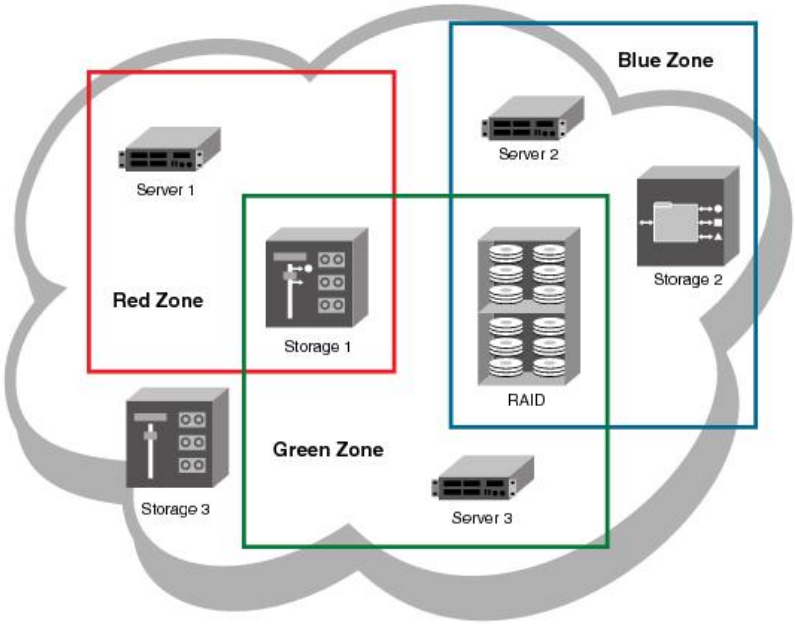

Abbildung 36: Zoning [NOSA_2014]

Das „fluten“ mit RCNS Events hätte nur noch Auswirkungen auf die jeweilige Zone.

M 4.3.3.2 – Unterdrücken von RSCNs Nachrichten auf Switch-Ebene

Einige FC-Switche ermöglichen es ausgewählte RSCN Events zu unterdrücken, sodass diese Änderungen nicht mehr den HBAs mitgeteilt werden. Andere Switche bieten die Möglichkeit die eintreffenden Events zu gruppieren und im reduzierten Umfang weiterzuleiten. Die jeweilige Implementierung hängt hierbei vom Switch-Hersteller ab. [FCAn_2006]

4.3.4 E-Port Replication

Hier gibt der Angreifer sich beim Zugriff auf die Fabric nicht als N-Port (Node-Port), sondern als E-Port (Expansion-Port) aus. Er imitiert somit einen Switch, der sich in die Fabric einbinden will. Der getäuschte Switch, sendet ihm automatisch Informationen, wie Zoning Tabellen oder Name Server Informationen zu, die daraufhin als kompromittiert betrachtet werden können. [Sto2003]

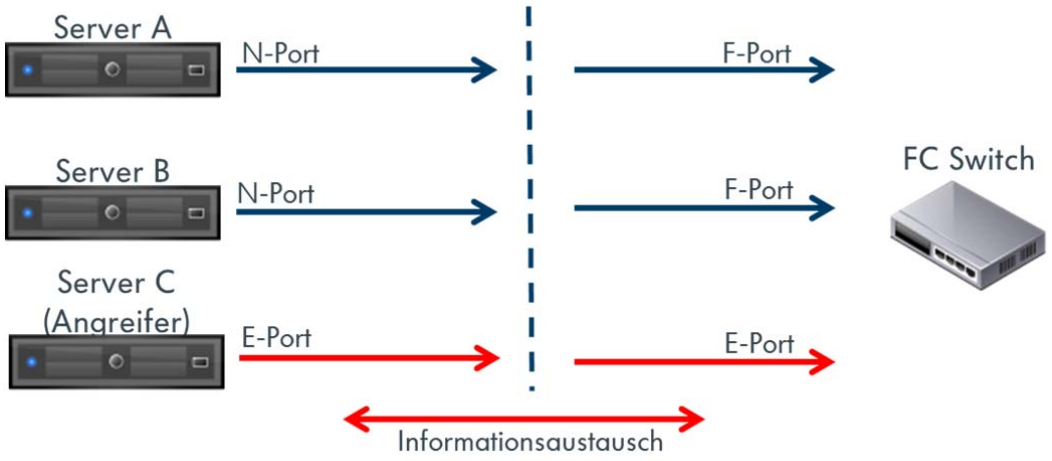

Abbildung 37: E-Ports Replication Attacke

Muss-Maßnahmen

M 4.3.4.1 - Absicherung unbenutzter Ports

Unbenutzte Ports der FC-Switche sollten grundsätzlich deaktiviert werden und in der Default-Einstellung auf „deaktiviert“ gesetzt werden. Somit wird verhindert, dass ein Angreifer unbemerkt offene Ports (zum Beispiel von noch nicht zurückgebauter SAN-Verkabelung) benutzt, um Zugriff auf die Fabric zu erlangen. [CSSE2011]

M 4.3.4.2 – Verwendung von Port Type Locking

Durch die Verwendung von Port Type Locking wird der Port Typ des FC-Switches fest vorgegeben. Der Default Port Typ wird von "Auto" auf "F-Port" umgestellt. So ist es einem kompromittierten Host zwar möglich sich als Switch auszugeben, er erhält aber keinen schreibenden Zugriff auf die Zoning-, Name- und Routing-Database. [CSSE2011]

4.4 Gefährdungen für das Zielobjekt „Speicher im Ethernet“

In diesem Kapitel werden Gefährdungen beschrieben, die Ethernet Speichersysteme betreffen.

Die unten beschriebenen Gefährdungen beschäftigen sich hierbei vorwiegend mit dem Zugriff auf fremde Storage Ressourcen, die durch die Vortäuschung falscher Identitäten entstehen.

4.4.1 Ausnutzen von "offenen" 802.1Q Trunks

Der Port des Switches wurde „fest“ für 802.1Q VLANs konfiguriert, die erlaubten VLANs wurden aber nicht eingeschränkt.

Bei diesem Angriff werden VLANs, die auf dem Switch konfiguriert sind, vom Server aber nicht benötigt werden, ausgenutzt um Zugriff auf fremde Ressourcen zu erlangen.

Hierbei kann der Angreifer leicht den Zugriff erlangen in dem er den richtigen VLAN Header verwendet. [CSSE2011]

Abbildung 38: Entfernung nicht notwendiger VLANs

Muss-Maßnahmen

M 4.4.1.1 - Entfernung nicht notwendiger VLANs

Die erlaubten VLANs sollten auf das Notwendigste bei jedem Access-Port eines Switches begrenzt werden. Jegliche für eine VM-Gast nicht notwendigen VLANs, wie Management, vMotion- oder IP-Storage VLANs sollte hier nicht anliegen.

4.4.2 IP Address Spoofing

Bei diesem Angriff versucht der Angreifer IP-Access-Listen bzw. Firewall Regeln zu umgehen, indem er sich eine falsche IP-Identität, d.h. eine falsche Quell-IP-Adresse gibt.

Wenn die Zugrifflisten eines NAS-Systems ausschließlich auf IP-Adressen basieren, kann der Angreifer dadurch den Zugriff auf Speicherbereiche erlangen, die ihm sonst verweigert werden. Zudem kann er auch DoS-Attacken gegen ein System fahren, das er anhand von IP-Access-Listen bzw. Firewall-Regeln eigentlich nicht erreichen sollte. [CSSE2011]

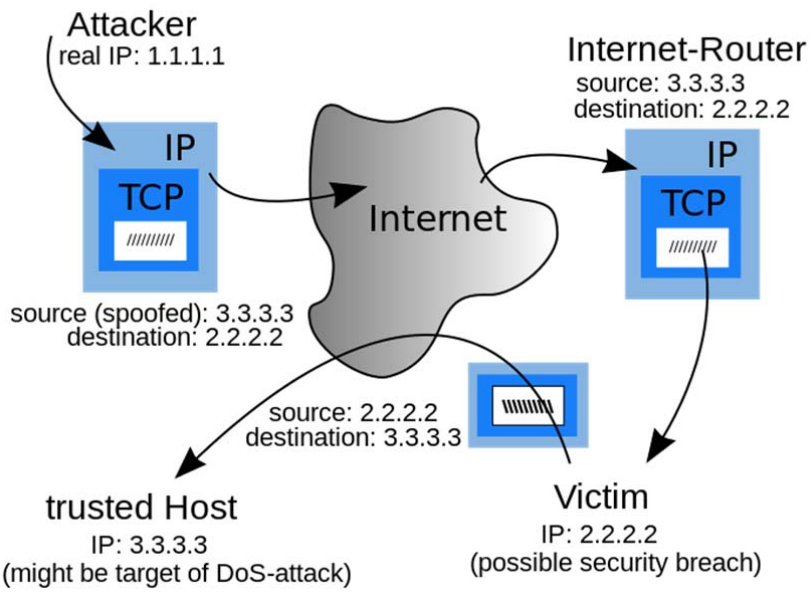

Abbildung 39: IP Address Spoofing [IPSp_2014]

Muss-Maßnahmen

M 4.4.2.1 – Validieren der Quell-IP-Adresse

Hierzu wird unter Einsatz der DHCP Snooping Binding Table geprüft, ob die Quell-IP-Adresse zum Absender passt. Eine falsche Quell-IP führt zum Verwurf des Paketes. [CSSE2011]

Siehe hierzu auch M 4.2.4.1 – Einsatz von DHCP Snooping

M 4.4.2.2 – Nutzung von vFilern und VLANs

Durch den Einsatz von vFilern kann der Zugriffsschutz auf Ebene des Netzes erhöht werden in dem ein einzelnes NAS System in mehrere NAS Geräte logisch getrennt wird. Mittels einer gespooften IP-Adresse ist dann nur noch der Zugriff auf den vFiler in dem entsprechenden Subnetz möglich. So sollte es pro Sicherheitsbereich einen eigenen vFiler geben. [BpfSN2007]

Abbildung 40: Netapp vFiler [vFil_2009]

4.4.2.3 – Implementierung von Kerberos Authentifikationsmechanismen

Um den Zugriffsschutz des NAS-Systems zu erhöhen ist es möglich Kerberos Authentifikationsmechanismen einzusetzen. Hierzu ist es notwendig, dass der Virtualisierungshost die Kerberos-Authentifikation unterstützt. Die Share Zugriffe sollten hierbei auf spezifische privilegierte Nutzer bzw. Gruppen begrenzt werden.

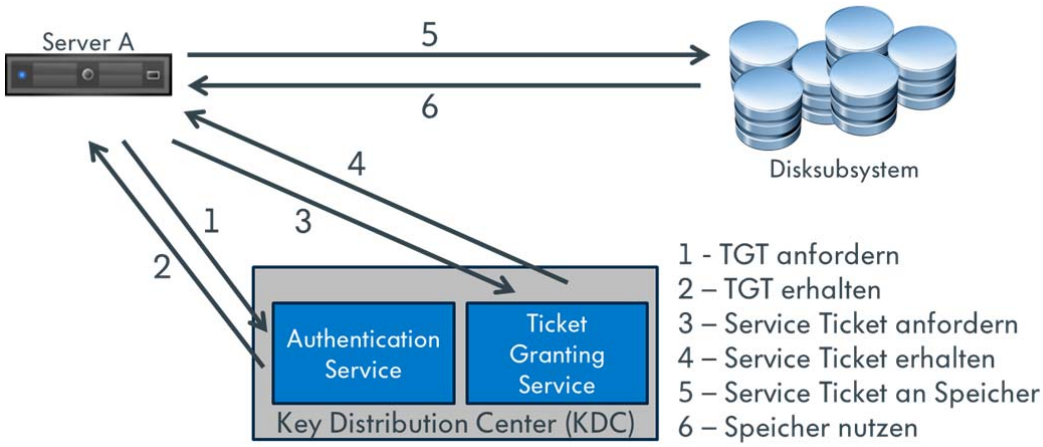

Abbildung 41: Die Funktionsweise von Kerberos

M 4.4.2.4 – Verschlüsselung der abgelegten Daten

Abhängig davon, auf welcher Ebene die Verschlüsselung der Daten ansetzt und abhängig davon, welche Authentifikationsmethode eingesetzt wird, lässt sich, durch die Verschlüsselung der Daten, das Risiko, dass unberechtigt auf Daten zugegriffen werden kann weiter reduzieren.

Die Verschlüsselung der Daten kann hierbei auf verschieden Ebenen ansetzen:
- Hostebene (Verschlüsselte Datenbank)
- SAN-Ebene
- Storage Subsystem

Bei der Verschlüsselung von abgelegten Daten ist auf Kosten und Nutzen zu achten. (wie z.B. durch die Risiken bei Verlust des Schlüssels, erhöhter Aufwand in der Administration etc.) [FCAn_2006]

4.5 Gefährdungen für das Zielobjekt „Speicher im Fibre Channel“

In diesem Kapitel werden Gefährdungen beschrieben, die Fibre Channel Speichersysteme betreffen.

Die unten beschriebenen Gefährdungen beschäftigen sich hierbei vorwiegend mit dem Zugriff auf fremde Storage Ressourcen, die durch die Vortäuschung falscher Identitäten entstehen.

4.5.1 WWN-Spoofing

Der Angreifer ersetzt die WWN (World Wide Number) seines Host-Bus-Adapters, durch die WWN eines anderen HBAs, um sich als dieser auszugeben. Dadurch erlangt er Zugriff auf Speicherbereiche, die ihm sonst verborgen bleiben. [CSSE2011]

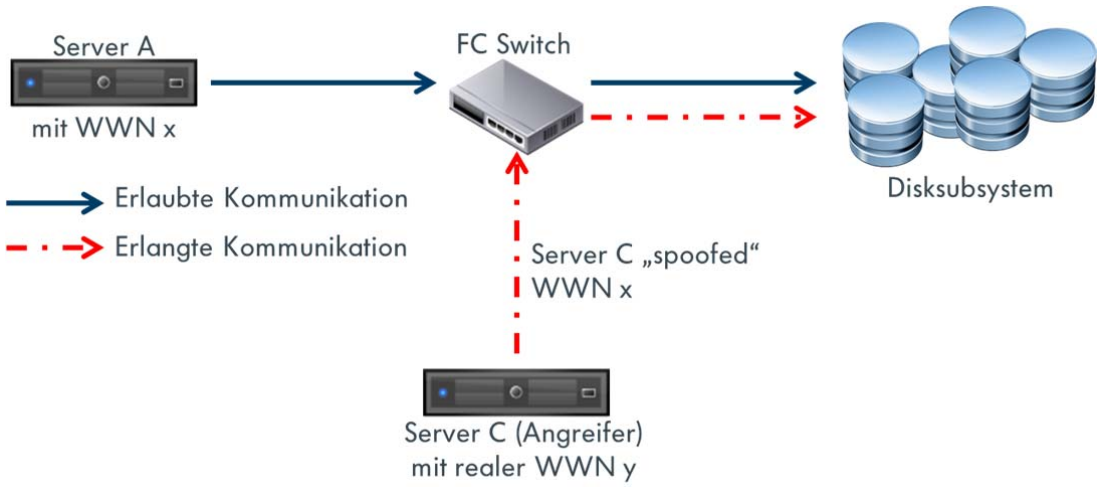

Abbildung 42: WWN Spoofing

Muss-Maßnahmen

M 4.5.1.1 – Verwendung von Physical Port Locking

Bei der Verwendung von Physical Port Locking wird die WWN eines HBAs fest einem FC Switch Port zugeordnet. [BpfSN2007]

M 4.5.1.2 – Verwendung von Port-Based Hard-Zoning

Das Port-Based Hard-Zoning verringert die Fehlerdomäne zusätzlich zur Bildung von vSANs um einen weiteren Faktor. An einen FibreChannel Switch angeschlossene HBAs können somit nur noch innerhalb ihrer Zone kommunizieren und auch nur noch die in ihrer Zone befindlichen anderen Ports erreichen. [FCAn_2006]

M 4.5.1.3 – Abweisen doppelter WWNs

Ein Sicherheitsfeature, dass viele FC-Switchhersteller anbieten, ist das Abweisen doppelter WWNs. Bevor sich ein HBA nun mit einer gefälschten WWN an der Fabric anmelden kann, muss er vorab den HBA mit der echten WWN dazu zwingen außer Dienst zu gehen. Dieser Umstand macht das WWN Spoofing um einiges komplizierter. [FCAn_2006]

M 4.5.1.4 – Verschlüsselung der abgelegten Daten

siehe M 4.4.2.4 – Verschlüsselung der abgelegten Daten [FCAn_2006]

M 4.5.1.4 - Nutzung von Authentifizierungsmechanismen

Nutzung von Authentifizierungsmechanismen zur Authentisierung am Speichersystem. Siehe hierzu M 4.2.8.1 [FCAn_2006]

M 4.5.1.5 – Konfiguration von LUN-Masking auf dem Storage Device

LUN Masking wird eingesetzt, um die Sichtbarkeit der Daten eines Speichersystems gegenüber den Servern festzulegen. Dem Datennutzer wird dadurch nur Zugriff auf Daten gewährt, für dessen Nutzung er auch berechtigt ist. [FCAn_2006]

5 Risikobewertung der einzelnen Gefährdungen

Die Risikobewertung pro Zielelement (Server, Netz, Speicher) wird anhand einer Auswirkungs-Wahrscheinlichkeits-Matrix durchgeführt und auf alle identifizierten Risiken aus dem vorangegangenen Kapitel angewendet.

Diese Technik ist im Projektmanagement eine Methode zur Bestimmung, ob die Auswirkungen eines Risikos als niedrig, mittel, hoch oder sehr hoch einzustufen sind. Dabei kombiniert die Methode die beiden Dimensionen eines Risikos. Die da wären:

- die Wahrscheinlichkeit des Eintretens
- de Auswirkungen im Falle des Eintretens [WuAm_2014]

		Eintrittswahrscheinlichkeit			
		Unwahr-scheinlich	Möglich	Wahrschein-lich	Sehr wahr-scheinlich
Schadenklasse	Sehr hoch	4	8	12	16
	Hoch	3	6	9	12
	Mittel	2	4	6	8
	Niedrig	1	2	3	4

Tabelle 3: Auswirkungs-Wahrscheinlichkeits-Matrix

Als Eingangsgrößen dienen die Ergebnisse des Kapitels „Identifikation der Gefährdungen und Risiken und Definition der Gegenmaßnahmen“. Das Ergebnis dieser Methode ist im Anschluss ein Risikoindex (1 bis 16) der sich aus dem jeweiligen Schaden und der Eintrittswahrscheinlichkeit ergibt.

Dabei sind definiert:
- Risikoindex von 1 bis 4: Risiko akzeptabel
- Risikoindex von 5 bis 11: Risiko gerade noch akzeptabel
- Risikoindex von 12 bis 16: Risiko inakzeptabel

Die beiden Dimensionen der Auswirkungs-Wahrscheinlichkeits-Matrix werden zudem wie folgt erweitert:

Die Betrachtung der Risiken wird für jede Gefährdung in Abhängigkeit der dazugehörigen Referenzarchitektur durchgeführt und auf die jeweilige Speicherlösung abgebildet. Zudem wird für jede Referenzarchitektur die Reduzierung des Risikoindexes nach Umsetzung der „Muss“ und „Kann“-Maßnahmen durchgeführt.

		REF 0	REF 1	REF2	REF 3
	Eintrittswahrscheinlich-keit	Sehr wahr-scheinlich	Unwahr-scheinlich	Unwahr-scheinlich	Unwahr-scheinlich
	Schadensklasse	Hoch	Mittel	Hoch	Sehr hoch
Risikoredu-zieriung	„Muss“-Maßnahmen:	-2	-2	-2	-2
	„Kann“-Maßnahmen:	-3	-3	-3	-3
NAS - Risi-ko-index	Nativ	12	2	3	4
	Nach "MUSS"	10	1	1	2
	Nach "KANN"	8	1	1	1

Tabelle 4: Vorlage Risikobewertung

Zu jeder Gefährdung werden nachfolgend die Eintrittswahrscheinlichkeit, die Schadenklasse und die Risikoreduzierung nach Umsetzung der Maßnahmen ausformuliert, da zu den identifizierten Schwachstellen keine Statistiken und praktischen Erfahrungsberichte in der entsprechenden Granularität vorhanden sind, auf die Bezug genommen werden könnte.

Generell lässt sich zur Eintrittswahrscheinlichkeit im Bereich von Fibre Channel Netzen sagen, dass, bis auf das WWN-Spoofing, sich alle Gefährdungen im Bereich des theoretisch möglichen befinden. Die möglichen Gefährdungen sind vom SANS Institute[15] und auf den BlackHat Briefings beschrieben worden. Es gibt keine öffentlichen verfügbaren Tools zur Ausnutzung dieser Schwachstellen. Die Fibre Channel Schwachstellen sind zudem nicht als Common Vulnerabilities and Exposures (CVE)[16] dokumentiert und bewertet.

Zudem arbeiten die Referenzarchitekturen 1 bis 3 mit einem dedizierten Speichernetz (im Gegensatz zur Referenzarchitektur 0). Dieser Umstand hat für alle Angriffe auf Switch und Speicherebene zur Folge, dass der Angreifer entweder den administrativen Zugang zu einem Server, der sich in diesem Netz befindet, erlangt oder direkt physikalischen Zugriff auf den entsprechenden Switch erlangt.

Die Referenzarchitektur 0 eignet sich nicht für den Einsatz in einem SAN und wird deshalb auch nicht in diesem Zusammenhang betrachtet.

[15] Beim SANS-Institut (SysAdmin, Networking and Security) handelt es sich um eine Genossenschaft, die sich vor allem im IT-Sicherheitsbereich einen Namen gemacht hat und jeweils die neueste Liste mit den Sicherheitslecks veröffentlicht. [SANS_2014]

[16] Common Vulnerabilities and Exposures (CVE) ist ein Industriestandard, dessen Ziel die Einführung einer einheitlichen Namenskonvention für Sicherheitslücken und andere Schwachstellen in Computersystemen ist. [CVS_2014]

5.1 Risikobewertung für das Zielobjekt „Server“

5.1.1 Virtual Machine Escape

Eintrittswahrscheinlichkeit:
Die Gefährdung durch das „Ausbrechen“ aus einer virtuellen Maschine und das damit einhergehende „Kapern“ des Hypervisors sind eher theoretischer Natur. Voraussetzung hierfür wären nicht nur, dass ausnutzen einer noch nicht bekannten Sicherheitslücke wie z.B. eines „Zero-Day-Exploits[17], sondern auch entsprechend tiefgehende Programmierkenntnisse bzw. Kenntnis des Hypervisors. Dass dieses Angriffsszenario aber durchaus realistisch ist, wurde bereits 2009 auf dem Blackhat[18] Briefing in Las Vegas gezeigt. [AvGt_2009] Die Eintrittswahrscheinlichkeit ist daher als „möglich“ einzustufen.
Schadenklasse:
Der Schaden, der durch das Ausnutzen dieser Sicherheitslücke entstehen kann, differiert zwischen „hoch“ (REF 0 und 1) und „sehr hoch“ (REF 2 und 3). Denn durch die Übernahme des Hypervisors hat der Angreifer zugriff auf alle Daten, die dem jeweiligen Hosts sichtbar sind und dieser potentielle Schaden ist umso höher einzustufen je mehr die Speicherarchitekturen konsolidiert werden. (REF 2 und REF3).
Risikoindex-Reduzierung nach Umsetzung der Maßnahmen:
Durch die Einführung des Patchmanagements und Umsetzung der Härtungsmaßnahmen der Hersteller sinkt die Eintrittswahrscheinlichkeit auf ein eher „unwahrscheinliches“ Maß. Dadurch sinkt der Risikoindex jeweils um vier bzw. drei Punkte.

		REF 0	REF 1	REF2	REF 3
	Eintrittswahrscheinlichkeit	Möglich	Möglich	Möglich	Möglich
	Schadensklasse	Hoch	Hoch	Sehr hoch	Sehr hoch
Risikoreduzieriung	„Muss“-Maßnahmen:	-3	-3	-4	-4
	„Kann“-Maßnahmen:	-	-	-	-
NAS - Risiko-index	Nativ	6	6	8	8
	Nach "MUSS"	3	3	4	4
	Nach "KANN"	3	3	4	4

Risikoreduzieriung	„Muss“-Maßnahmen:		-3	-4	-4
	„Kann“-Maßnahmen:		-	-	-
SAN - Risiko-index	Nativ		6	8	8
	Nach "MUSS"		3	4	4
	Nach "KANN"		3	4	4

Tabelle 5: Risikobewertung - Virtual Machine Escape

[17] Ein Zero-Day-Exploit nutzt eine Schwachstelle aus noch bevor Sie dem Softwarehersteller gemeldet wurde.

[18] Blackhat ist der Name einer Konferenz zur Informationssicherheit

5.1.2 Überbuchung von Speicherressourcen

Eintrittswahrscheinlichkeit:

Die Überbuchung von Speicherressourcen ist eine durchaus wahrscheinliche Angriffsmöglichkeit. Hierzu ist nur der Zugriff auf eine virtuelle Maschine notwendig. Dies kann durch einen externen Angreifer geschehen, der eine Sicherheitslücke ausnutzt oder durch einen internen Angreifer, der den vollen Zugriff auf die virtuelle Maschine hat.

Schadenklasse:

Der Schaden der durch diesen Angriff verursacht werden kann ist als „mittel“ einzustufen. Denn die Auswirkung betrifft „nur“ den Speicher auf dem die virtuelle Maschine abgelegt ist und ist über alle Referenzarchitekturen als gleich zu betrachten.

Risikoindex-Reduzierung nach Umsetzung der Maßnahmen:

Durch das Festlegen und Überwachen der maximalen Ressourcen, sinkt die Eintrittswahrscheinlichkeit der Überfüllung einer LUN auf ein „mögliches“ Maß und die Auswirkungen sinken auf ein „niedriges“ Niveau, da sie quasi nur noch die virtuelle Maschine betreffen. Durch die Umsetzung der „Kann“-Maßnahmen sinkt die Eintrittswahrscheinlichkeit auf „unwahrscheinlich“. Der Risikoindex reduziert sich dadurch um 4 Punkte bzw. 5 Punkte.

		REF 0	REF 1	REF2	REF 3
	Eintrittswahrscheinlichkeit	Wahrscheinlich	Wahrscheinlich	Wahrscheinlich	Wahrscheinlich
	Schadensklasse	Mittel	Mittel	Mittel	Mittel
Risikoreduzierung	„Muss“-Maßnahmen:	-4	-4	-4	-4
	„Kann“-Maßnahmen:	-4	-4	-4	-4
NAS - Risiko-index	Nativ	6	6	6	6
	Nach "MUSS"	4	4	4	4
	Nach "KANN"	2	2	2	2
Risikoreduzierung	„Muss“-Maßnahmen:		-4	-4	-4
	„Kann“-Maßnahmen:		-4	-4	-4
SAN - Risiko-index	Nativ		6	6	6
	Nach "MUSS"		4	4	4
	Nach "KANN"		2	2	2

Tabelle 6: Risikobewertung - Überbuchung von Speicherressourcen

5.1.3 Fehler im Bandbreitenmanagement

Eintrittswahrscheinlichkeit:

Die Eintrittswahrscheinlichkeit für Fehler im Bandbreitenmanagement ist genau so wahrscheinlich wie die Überbuchung von Speicherressourcen.

Schadenklasse:

Die Auswirkungen differieren in Abhängigkeit von der Referenzarchitektur. Bei REF 0 haben Fehler im Bandbreitenmanagement auch Auswirkungen auf die Anbindung der virtuellen Maschinen, die Schadenklasse ist daher als „hoch“ zu betrachten. Durch die strikte Segmentierung der REF 1 sinkt die Schadenklasse auf „mittel“, die Konsolidierungen der REF 2 und REF 3 haben dagegen als Auswirkung, dass die Schadenklasse auf „hoch“ bzw. „sehr hoch“ steigt, da Bandbreitenüberbuchungen das ganze Speichersystem betreffen können.

Risikoindex-Reduzierung nach Umsetzung der Maßnahmen:

Durch die Umsetzung der Maßnahmen zur Bandbreitenreduzierung können die Risiken aber effektiv auf ein „mittleres und mögliches“ Maß gesenkt werden

		REF 0	REF 1	REF2	REF 3
	Eintrittswahrscheinlichkeit	Wahrscheinlich	Wahrscheinlich	Wahrscheinlich	Wahrscheinlich
	Schadensklasse	Sehr hoch	Mittel	Hoch	Sehr hoch
Risikoreduzierung	„Muss“-Maßnahmen:	-4	-4	-4	-4
	„Kann“-Maßnahmen:	-4	-4	-4	-4
NAS - Risiko-index	Nativ	12	6	9	12
	Nach "MUSS"	4	4	4	4
	Nach "KANN"	4	4	4	4
Risikoreduzierung	„Muss“-Maßnahmen:		-4	-4	-4
	„Kann“-Maßnahmen:		-4	-4	-4
SAN - Risiko-index	Nativ		6	9	12
	Nach "MUSS"		4	4	4
	Nach "KANN"		4	4	4

Tabelle 7: Risikobewertung - Fehler im Bandbreitenmanagement

5.1.4 Unautorisiertes Mitlesen oder Stören des Virtualisierungsnetzes durch unzureichende Trennung von Mandanten und internen Netzen

Eintrittswahrscheinlichkeit:

Durch eine unzureichende Trennung von Internen- und Mandantennetzen kann es zu unautorisiertem Mitlesen oder Stören des Virtualisierungsnetzes kommen. Dieser Angriff ist nur bei der Referenzarchitektur 0 möglich. Die weiteren Referenzarchitekturen sehen einen getrennten Aufbau von Speicher- und Mandantennetz vor. Die Eintrittswahrscheinlichkeit ist hierbei als „wahrscheinlich“ einzustufen, da ein Netzwerkanalyser ausreichen würde, um den Datenverkehr mitzuschneiden.

Schadenklasse:

Die Schadenklasse ist als „sehr hoch“ einzustufen.

		REF 0	REF 1	REF2	REF 3
	Eintrittswahrscheinlich-keit	Wahrschein-lich	-	-	-
	Schadensklasse	Sehr hoch	-	-	-
Risikoredu-zieriung	„Muss“-Maßnahmen:	-8			
	„Kann“-Maßnahmen:	-10			
NAS - Risi-ko-index	Nativ	12			
	Nach "MUSS"	4			
	Nach "KANN"	2			

Tabelle 8: Risikobewertung - Unautorisiertes Mitlesen oder Stören des Virtualisierungsnetzes durch unzureichende Trennung von Mandanten und internen Netzen im Bereich NAS

Risikoindex-Reduzierung nach Umsetzung der Maßnahmen:

Nach Umsetzung der „Muss“-Maßnahme, der logischen Trennung der Netze, sinkt die Eintrittswahrscheinlichkeit auf ein „mögliches“ Maß. Da das Mitlesen nur noch beim Überspringen eines VLANs möglich ist. Nach der Umsetzung der „Kann“-Maßnahme, physikalische Trennung, sinkt die Eintrittswahrscheinlichkeit auf ein „unwahrscheinliches“ Maß. Die Auswirkungen sind weiterhin als „sehr hoch“ zu betrachten.

Der Protokollunterschied von SAN führt zwangsweise zu einer Trennung von Mandanten und Speichernetzen. Die Gefahr von unautorisiertem Mitlesen oder Stören des Netzes aus dem Mandantennetz ist hier ausgeschlossen.

5.2 Risikobewertung für das Zielobjekt „Ethernet Switch“

Kapitel 5.2 führt die Risikobewertung für das Zielobjekt „Ethernet Switch“ durch. Die Risikobewertung wird hierbei aus Sicht der korrumpierten virtuellen Maschine, Hypervisors oder direktem Netzzugriff in Richtung des Speichers durchgeführt.

5.2.1 MAC Flooding

Eintrittswahrscheinlichkeit:
Die Eintrittswahrscheinlichkeit für das MAC Flooding, also das Überfluten des Netzswitches, ist bei REF0 ein wahrscheinliches Szenario, da die Mandanten und der Speicher sich die gleiche Infrastruktur teilen.

Bei REF1 bis REF3 ist die Wahrscheinlichkeit des Eintretens als „möglich“ zu betrachten. Dies setzt den Zugang zu einem Hypervisor voraus oder den Zugriff auf das Netz in dem sich die Speichergeräte befinden.

Schadenklasse:
Die Schadenklasse differiert bei den unterschiedlichen Referenzarchitekturen, REF1 und 2 haben für die unterschiedlichen Sicherheitsniveaus eigene Switche. Die Auswirkungen sind hier als „hoch“ zu betrachten. REF3 nutzen einen Switch für alle Sicherheitsniveaus. Die möglichen Auswirkungen sind hier als „sehr hoch“ zu betrachten. Bei REF 0 hätte das Fluten der Netzswitche auch Auswirkungen auf die Mandanten und daher sind auch hier die Auswirkungen als „sehr hoch“ zu betrachten.

Risikoindex-Reduzierung nach Umsetzung der Maßnahmen:
Die konsequente Zuordnung der MAC-Adressen zu den Netzwerkports führt zu einer Reduzierung der Eintrittswahrscheinlichkeit auf ein „unwahrscheinliches“ Maß. Die Umsetzung der „KANN“-Maßnahmen hat keine weiteren Auswirkungen auf die Eintrittswahrscheinlichkeit. Die Schadenklassen bleiben unverändert.

		REF 0	REF 1	REF2	REF 3
	Eintrittswahrscheinlichkeit	Wahrscheinlich	Möglich	Möglich	Möglich
	Schadensklasse	Sehr hoch	Hoch	Hoch	Sehr hoch
Risikoreduzierung	„Muss“-Maßnahmen:	-8	-2	-2	-3
	„Kann“-Maßnahmen:	-8	-2	-2	-3
NAS - Risiko-index	Nativ	12	6	6	8
	Nach "MUSS"	4	3	3	4
	Nach "KANN"	4	3	3	4

Tabelle 9: Risikobewertung – MAC Flooding

5.2.2 MAC Spoofing

Eintrittswahrscheinlichkeit:

Beim MAC-Spoofing kann, durch Änderung der MAC-Adressen zu Port Zuordnung im Switch, eine Man-in-the-Middle Attacke erfolgen. Wie schon beim MAC- Flooding ist die Eintrittswahrscheinlichkeit bei der Referenzarchitektur 0 auf Grund der gleichen Infrastruktur als „wahrscheinlich“ zu bewerten.

Schadenklasse:

Sollt es einem Angreifer gelingen sich als Man-In-The-Middle zu etablieren, ist es ihm möglich den Datenverkehr mitzulesen, aber auch zu verändern. Der Schaden hierbei ist über alle Referenzarchitekturen 0 bis 2 als gleichwertig „hoch“ zu betrachten, die Referenzarchitektur 3 ist auf Grund der stark konsolidierten Sicherheitsniveaus als besonders kritisch zu betrachten.

Risikoindex-Reduzierung nach Umsetzung der Maßnahmen:

Die konsequente Zuordnung der MAC-Adressen zu den Netzwerkports führt zu einer Reduzierung der Eintrittswahrscheinlichkeit auf ein „unwahrscheinliches“ Maß. Die Umsetzung der „KANN“-Maßnahmen hat keine weiteren Auswirkungen auf die Eintrittswahrscheinlichkeit. Die Schadenklassen bleiben unverändert.

		REF 0	REF 1	REF2	REF 3
	Eintrittswahrscheinlichkeit	Wahrscheinlich	Möglich	Möglich	Möglich
	Schadensklasse	Hoch	Hoch	Hoch	Sehr hoch
Risikoreduzierung	„Muss“-Maßnahmen:	-6	-3	-3	-3
	„Kann“-Maßnahmen:	-6	-3	-3	-3
NAS - Risiko-index	Nativ	9	6	6	8
	Nach "MUSS"	3	3	3	4
	Nach "KANN"	3	3	3	4

Tabelle 10: Risikobewertung - MAC Spoofing

5.2.3 Spanning Tree Angriffe

Eintrittswahrscheinlichkeit:

Auf der Blackhat Convention 2005 wurde das Tool „Yersinia“ vorgestellt, hiermit ist es unter anderem möglich STP Attacken über ein GUI durchzuführen. Die Verfügbarkeit solch vorgefertigter Tools führt dazu, dass theoretisch durchführbare Angriffe, somit praktisch leicht umsetzbar werden. Die Eintrittswahrscheinlichkeit dies, in Bezug auf das Speichernetz, durchzuführen ist bei der Referenzarchitektur 0 am größten. Für die weiteren Referenzarchitekturen ist diese Angriffsart möglich. Setzt aber den vorher erlangten Netzzugang über den Hypervisor oder den physikalischen Zugang zum Switch voraus. [Yers_2005]

Schadenklasse:

Die Schadenklasse ist bei der Referenzarchitektur 0 und 3 am höchsten, da hier eine gemeinsame Switch-Infrastruktur je Sicherheitsbereich verwendet wird. Veränderungen der Spanning Tree Topologie würden das gesamte Netz betreffen, daher sind die Auswirkungen als „sehr hoch“ zu beziffern. Die Referenzarchitekturen 1 und 2 nutzen hier je Sicherheitsniveau eigene Netztechnik. Die Fehlerdomänen sind dementsprechend kleiner. Die Auswirkungen, zum Beispiel durch eine Schleife, sind aber dennoch als „hoch“ zu betrachten.

Risikoindex-Reduzierung nach Umsetzung der Maßnahmen:

Durch die Einführung der „Muss“-Maßnahmen kann die Wahrscheinlichkeit des Eintretens von STP-Attacken auf ein „unwahrscheinliches“ Niveau reduziert werden, da die BDPU Frames von Access Ports geblockt werden.

		REF 0	REF 1	REF2	REF 3
	Eintrittswahrscheinlichkeit	Wahrscheinlich	Möglich	Möglich	Möglich
	Schadensklasse	Sehr hoch	Hoch	Hoch	Sehr hoch
Risikoreduzierung	„Muss“-Maßnahmen:	-8	-3	-3	-4
	„Kann“-Maßnahmen:	-8	-3	-3	-4
NAS - Risiko-index	Nativ	12	6	6	8
	Nach "MUSS"	4	3	3	4
	Nach "KANN"	4	3	3	4

Tabelle 11: Risikobewertung - Spanning Tree Angriffe

5.2.4 IP Session Hijacking

Eintrittswahrscheinlichkeit:

Für Attacken wie das IP Session Hijacking gibt es vorgefertigte Applikationen, die diese Angriffsart problemlos ermöglichen. Hier wäre z.B. das Programm „Hunt“ zu nennen mit dem Telnet-Sitzungen übernommen werden können. [Sec2005] Die freie Verfügbarkeit solcher Programme macht die Eintrittswahrscheinlichkeit solcher Angriffe gerade bei der REF0 „wahrscheinlich“. Die Referenzarchitekturen 1 bis 3 haben hier wieder den Vorteil, dass der Zugriff auf das Speichernetz nicht direkt aus einer VM heraus, sondern nur über den Hypervisor bzw. einen direkten Speichernetzzugang möglich ist. Die Möglichkeit solch eines Angriffs ist daher nicht unwahrscheinlich, aber möglich.

Schadenklasse:

Unabhängig von der Referenzarchitektur kann das IP-Session Hijacking als kritischer Angriff mit hohem Schadenpotential angesehen werden, da dadurch Authentifikationsmechanismen einfach umgangen werden können und ein unautorisierter Angreifer so den Zugriff auf sensible Daten erlangen kann. Das IP-Session Hijacking birgt für die REF3 das höchste Gefahrenpotential, da hier unterschiedliche Sicherheitsniveaus zusammengefasst wurden.

Risikoindex-Reduzierung nach Umsetzung der Maßnahmen:

Die Umsetzung der „Muss“-Maßnahme und damit die Einführung von IPsec verhindert effektiv das IP Session Hijacking. Die Sequenznummer jedes Paketes wird dadurch verschlüsselt und ist nicht mehr vorhersehbar. Das Eintreten dieser Gefährdung wird dadurch unwahrscheinlich.

		REF 0	REF 1	REF2	REF 3
	Eintrittswahrscheinlichkeit	Wahrscheinlich	Möglich	Möglich	Möglich
	Schadensklasse	Hoch	Hoch	Hoch	Sehr hoch
Risikoreduzierung	„Muss“-Maßnahmen:	-6	-3	-3	-4
	„Kann“-Maßnahmen:	-6	-3	-3	-4
NAS - Risiko-index	Nativ	9	6	6	8
	Nach "MUSS"	3	3	3	4
	Nach "KANN"	3	3	3	4

Tabelle 12: Risikobewertung - IP Session Hijacking

5.2.5 Double-Encapsulated 802.1Q / Nested VLAN Attack

Eintrittswahrscheinlichkeit:

Das Eintreten dieser Angriffsvariante ist nur unter folgenden Bedingungen möglich:

- Auf dem Netz-Port, der dem Angreifer zur Verfügung steht muss ein VLAN vorhanden sein.
- Es muss VLAN ID = 0 oder VLAN ID = VLAN ID des Access-Ports verwendet werden, da sonst das Paket vom Switch verworfen wird.
- Auf dem 802.1Q VLAN Trunk zu dem Angreifer muss das gleiche VLAN verfügbar sein, welches als natives VLAN auf den Trunks im Backbone zwischen den Switchen konfiguriert ist. [CSSE2011] S.57

Die Kombination dieser Notwendigkeiten macht einen Angriff zwar möglich, aber nicht wahrscheinlich.

Schadenklasse:

Der mögliche Schaden bei diesem Angriff ist auf eine DoS-Attacke begrenzt, da nur Pakete gesendet, aber nicht empfangen werden können. Der Schaden ist im Vergleich zu anderen Attacken als „mittel“ zu betrachten.

Risikoindex-Reduzierung nach Umsetzung der Maßnahmen:

Durch das Abstellen, einer der oben genannten Gegebenheiten, kann der Angriff nicht mehr durchgeführt werden und das Eintreten dieser Attacke wird „unwahrscheinlich“.

		REF 0	REF 1	REF2	REF 3
	Eintrittswahrscheinlichkeit	Möglich	Möglich	Möglich	Möglich
	Schadensklasse	Mittel	Mittel	Mittel	Mittel
Risikoreduzierung	„Muss“-Maßnahmen:	-2	-2	-2	-2
	„Kann“-Maßnahmen:	-2	-2	-2	-2
NAS - Risiko-index	Nativ	4	4	4	4
	Nach "MUSS"	2	2	2	2
	Nach "KANN"	2	2	2	2

Tabelle 13: Risikobewertung - Double-Encapsulated 802.1Q / Nested VLAN Attack

5.2.6 ARP Spoofing

Eintrittswahrscheinlichkeit:

ARP Spoofing ist bereits mit geringen technischen Kenntnissen anwendbar. Ein weit verbreitetes Hacker-Tool, um diese Angriffsart durchzuführen, ist Cain & Abel. Hiermit ist es möglich den Datenverkehr des gewünschten Teilnehmers in einem Subnetz mitzulesen. Wie schon beim MAC Flooding und Spoofing ist die Eintrittswahrscheinlichkeit bei der Referenzarchitektur 0 am wahrscheinlichsten. Die Attacke ist auch bei den weiteren Referenzarchitekturen anwendbar, aber mit einem höheren Aufwand verbunden.

Schadenklasse:

Bei ARP Angriffen ist der Schaden auf das jeweilige Subnetz begrenzt in dem sich der Angreifer befindet, da ARP auf Ebene 2 des OSI-Schichtenmodells arbeitet. Da der Einsatz dieser Attacke „Man-In-The-Middle“-Attacken ermöglicht ist der potentielle Schaden der durch den Zugriff oder die Manipulation entstehen kann über die Referenzarchitekturen als „hoch“ anzusehen. Wie bereits bei den zuvor betrachteten Gefährdungen, birgt die REF3, das höchste Gefahrenpotential, da hier unterschiedliche Sicherheitsniveaus zusammengefasst wurden.

Risikoindex-Reduzierung nach Umsetzung der Maßnahmen:

Die Umsetzung der definierten „Muss“-Maßnahmen, wie z.B. der Einsatz von DHCP-Snooping Mechanismen, unterbindet ARP Angriffe, da Pakete mit falscher IP zu MAC-Zuordnung verworfen werden. Zudem verkleinern sich die Fehlerdomänen bei der Bildung von VLANs und die Schadenklassen sinken auf ein „mittleres“ Niveau. Die Umsetzung der „Kann“-Maßnahmen erhöht die Sicherheit nicht merklich.

		REF 0	REF 1	REF2	REF 3
	Eintrittswahrscheinlichkeit	Wahrscheinlich	Möglich	Möglich	Möglich
	Schadensklasse	Hoch	Hoch	Hoch	Sehr hoch
Risikoreduzierung	„Muss“-Maßnahmen:	-7	-4	-4	-4
	„Kann“-Maßnahmen:	-7	-4	-4	-4
NAS - Risiko-index	Nativ	9	6	6	8
	Nach "MUSS"	2	2	2	2
	Nach "KANN"	2	2	2	2

Tabelle 14: Risikobewertung - ARP Spoofing

5.3 Risikobewertung für das Zielobjekt „FC Switch“

Kapitel 5.3 führt die Risikobewertung für das Zielobjekt „FC Switch“ durch. Die Risikobewertung wird hierbei aus Sicht der korrumpierten virtuellen Maschine, Hypervisors oder direktem Netzzugriff in Richtung des Speichers durchgeführt.

Es werden dabei nur die Referenzarchitekturen 1 bis 3 betrachtet, da ein Aufbau in der Referenzarchitektur 0 mit SAN nicht möglich ist.

5.3.1 FC Session Hijacking

Eintrittswahrscheinlichkeit:
Im Gegensatz zum IP Session Hijacking gibt es keine frei verfügbaren Tools, die ein automatisches FC Session Hijacking ermöglichen. Trotz dessen ist das Angriffsszenario als möglich anzusehen, da die Protokollschwächen im FC Protokoll existieren. [Sec2005]

Schadenklasse:
Genau wie das IP Session Hijacking kann das FC Session Hijacking, unabhängig von der Referenzarchitektur, als kritischer Angriff mit hohem Schadenpotential angesehen werden, da dadurch Authentifikationsmechanismen einfach umgangen werden können und ein unautorisierter Angreifer so den Zugriff auf sensible Daten erlangen kann. Für die Referenzarchitektur 3 ist das Gefahrenpotential am höchsten, da hier unterschiedliche Sicherheitsniveaus zusammengefasst wurden.

Risikoindex-Reduzierung nach Umsetzung der Maßnahmen:
Durch Einführung von FCsec kann die Authentizität jedes Frames sichergestellt und die Datenherkunft festgestellt werden. Die Sequence Control Number und Sequence Identifcation Number jedes Paketes werden dadurch verschlüsselt und sind nicht mehr vorhersehbar. Das Eintreten dieser Gefährdung wird dadurch unwahrscheinlich.

		REF 0	REF 1	REF2	REF 3
	Eintrittswahrscheinlichkeit		Möglich	Möglich	Möglich
	Schadensklasse		Hoch	Hoch	Sehr hoch
Risikoreduzierung	„Muss“-Maßnahmen:		-3	-3	-3
	„Kann“-Maßnahmen:		-3	-3	-3
SAN - Risiko-index	Nativ		6	6	8
	Nach "MUSS"		3	3	4
	Nach "KANN"		3	3	4

Tabelle 15: Risikobewertung - FC Session Hijacking

5.3.2 Name Server Pollution

Eintrittswahrscheinlichkeit:

Um die Name Server Pollution Attacke durchführen zu können, benötigt man nicht nur den Zugriff auf einen Hosts mit Verbindung zum SAN, sondern auch noch tiefgehende Kenntnisse in Bezug auf den HBA Treiber, der in so weit modifiziert werden muss, dass er die gefälschten PLOGI Frames versendet. Dies macht den Angriff entsprechend kompliziert, aber nicht unmöglich.

Schadenklasse:

Der Schaden der durch diesen Angriff entstehen kann, ist als „hoch“ zu klassifizieren. Der Angreifer kann mit sich mit dieser Attacke als Man-in-the-Middle etablieren und so den Zugriff auf Ressourcen erlangen, die ihm vorher verwehrt geblieben sind. Der mögliche Schaden ist bei der Referenzarchitekturen 3 am gravierendsten, da hier unterschiedliche Sicherheitsniveaus auf einer gemeinsamen Plattform betrieben werden.

Risikoindex-Reduzierung nach Umsetzung der Maßnahmen:

Nach der Umsetzung der „Muss“-Maßnahmen werden Änderungen in der Name Server Datenbank nur noch von Teilnehmer durchgeführt, die vorab ihre Identität nachgewiesen haben. Die Eintragung gefälschter Werte wird dadurch ausgeschlossen. Die Eintrittswahrscheinlichkeit sinkt auf ein „unwahrscheinliches“ Maß. Zudem verringert die Bildung von vSANs die Fehlerdomäne. Der mögliche Schaden verringert sich dadurch auf ein „mittleres Niveau“.

		REF 0	REF 1	REF2	REF 3
	Eintrittswahrscheinlichkeit		Möglich	Möglich	Möglich
	Schadensklasse		Hoch	Hoch	Sehr hoch
Risikoreduzierung	„Muss“-Maßnahmen:		-4	-4	-4
	„Kann“-Maßnahmen:		-4	-4	-4
SAN - Risiko-index	Nativ		6	6	8
	Nach "MUSS"		2	2	2
	Nach "KANN"		2	2	2

Tabelle 16: Risikobewertung - Name Server Pollution

5.3.3 Reconfigure Fabric Attack

Eintrittswahrscheinlichkeit:
Es gibt verschiedene Wege um die Reconfigure Fabric Attacke durchzuführen. Die wohl einfachste ist es den Host Bus Adapters, über den ein Angreifer die Kontrolle hat, kontinuierlich und in schneller Abfolge, in einen „offline“ und „online“ Status zu versetzen. Dies wird zwar auch den HBA des Angreifers nicht funktionsfähig machen. Ist aber ausreichend für eine DoS-Attacke. Die Eintrittswahrscheinlichkeit dies, in Bezug auf das Speichernetz, durchzuführen ist bei der Referenzarchitektur 1 bis 3 möglich. Setzt aber den vorher erlangten Netzzugang über den Hypervisor oder den physikalischen Zugang zum Switch voraus. [FCAn_2006]

Schadenklasse:
Die Schadenklasse dieses Angriffs steigt mit der Größe der Fehlerdomäne. Da die Referenzarchitekturen 1 und 2 noch getrennte Switche je Sicherheitsniveau einsetzen, ist der mögliche Schaden hier zwar noch „hoch“, aber noch geringer als bei der Referenzarchitektur 3 bei der für alle Sicherheitsniveaus die gleich Fabric verwendet wird und der mögliche Schaden hier als „sehr hoch“ bewertet werden kann.

Risikoindex-Reduzierung nach Umsetzung der Maßnahmen:
Durch die Gruppierungs- und teilweisen Unterdrückungsmechanismen, die sich auf Switch-Ebene für Registered State Change Notifications implementieren lassen ist es möglich die Eintrittswahrscheinlichkeit der Reconfigure Fabric Attacke zumindest auf ein unwahrscheinliches Maß zu reduzieren. Die Risiken gänzlich zu minimieren ist nicht möglich, da die Notifications schließlich für die Anzeige von fehlerhaften Zuständen ihre Daseinsberechtigung haben. Durch den Einsatz von Zoning lässt sich die Fehlerdomäne weiter verringern, sodass die DoS-Attacke nur noch Auswirkungen in der jeweiligen Zone des Angreifers hat.

		REF 0	REF 1	REF2	REF 3
	Eintrittswahrscheinlichkeit		Möglich	Möglich	Möglich
	Schadensklasse		Hoch	Hoch	Sehr hoch
Risikoreduzierung	„Muss“-Maßnahmen:		-4	-4	-4
	„Kann“-Maßnahmen:		-4	-4	-4
SAN - Risiko-index	Nativ		6	6	8
	Nach "MUSS"		2	2	4
	Nach "KANN"		2	2	4

Tabelle 17: Risikobewertung - Reconfigure Fabric Attack

5.3.4 E-Port Replication

Eintrittswahrscheinlichkeit:

Um diesen Angriff durchführen zu können müsste der Angreifer entweder physikalischen Zugriff zu einem freien FC-Port erlangen, an den er seinen eigenen FC-Switch anschließen würde oder es müsste ihm gelingen seinen HBA so umzuprogrammieren, sodass dieser sich als E-Port ausgibt. Die Eintrittswahrscheinlichkeit bei dieser Attacke ist eher unwahrscheinlich, aber möglich.

Schadenklasse:

Sollte es einem Angreifer gelingen sich als Switch auszugeben bzw. seinen FC-Switch mit der Fabric zu verbinden, kann er über die E-Port Replication an alle Information der Fabric gelangen. Nameserver, Management und Zoning Tabellen könnten somit als korrumpiert betrachtet werden. Der mögliche Schaden, den ein Angreifer mit diesen Informationen anrichten könnte, wäre sehr hoch.

Risikoindex-Reduzierung nach Umsetzung der Maßnahmen:

Die Abschaltung unbenutzter Ports und das deaktivieren der automatischen Port-Type-Vergabe verhindern effektiv die E-Port Replikation.

		REF 0	REF 1	REF2	REF 3
	Eintrittswahrscheinlich-keit		Möglich	Möglich	Möglich
	Schadensklasse		Sehr hoch	Sehr hoch	Sehr hoch
Risikoredu-zieriung	„Muss“-Maßnahmen:		-4	-4	-4
	„Kann“-Maßnahmen:				
SAN - Risi-ko-index	Nativ		8	8	8
	Nach "MUSS"		4	4	4
	Nach "KANN"		4	4	4

Tabelle 18: Risikobewertung - E-Port Replication

5.4 Risikobewertung für das Zielobjekt „Speicher im Ethernet“

5.4.1 Ausnutzen von "offenen" 802.1Q Trunks

Eintrittswahrscheinlichkeit:
Das Eintreten dieses Fehlers basiert nicht auf einer bestehenden Schwachstelle oder einer Sicherheitslücke, sondern auf menschlichem bzw. organisatorischem Versagen. Das Auftreten solch eines Konfigurationsfehlers ist aber durch aus möglich.

Schadenklasse:
Die Schadenklasse ist bei den Referenzarchitekturen 0 und 3 auf Grund der gemeinsamen Switch-Infrastruktur höher, da potentiell mehr offene VLANs zur Verfügung stehen könnten. Zudem sind bei der Referenzarchitektur 3 mehrere Sicherheitsniveaus auf einer physikalischen Switch-Hardware vereint. Der potentielle Schaden ist hier dementsprechend als sehr hoch zu bewerten.

Risikoindex-Reduzierung nach Umsetzung der Maßnahmen:
Durch Einführung entsprechender organisatorischer Maßnahmen, wie z.B. das Monitoren von Konfigurationssettings, machen diesen Fehler eher unwahrscheinlich.

		REF 0	REF 1	REF2	REF 3
	Eintrittswahrscheinlichkeit	Möglich	Möglich	Möglich	Möglich
	Schadensklasse	Sehr hoch	Hoch	Hoch	Sehr hoch
Risikoreduzierung	„Muss“-Maßnahmen:	-4	-3	-3	-4
	„Kann“-Maßnahmen:	-4	-3	-3	-4
NAS - Risiko-index	Nativ	8	6	6	8
	Nach "MUSS"	4	3	3	4
	Nach "KANN"	4	3	3	4

Tabelle 19: Risikobewertung - Ausnutzen von "offenen" 802.1Q Trunks

5.4.2 IP-Address Spoofing

Eintrittswahrscheinlichkeit:

Wie für die meisten anderen IP-basierten Angriffe, gibt es auch für IP-Adress Spoofing vorgefertigte Tools, die hierfür genutzt werden können und nicht extra geschrieben werden müssen. Die Referenzarchitekturen 1 bis 3 haben hier wieder den Vorteil, dass der Zugriff auf das Speichernetz nicht direkt aus einer VM heraus, sondern nur über den Hypervisor bzw. einen direkten Speichernetzzugang möglich ist. Die Möglichkeit solch eines Angriffs ist daher nicht unwahrscheinlich, aber möglich.

Schadenklasse:

Das IP Address Spoofing ermöglicht es dem Angreifer Zugriff auf Ressourcen zu erlangen, die ihm vorher verwehrt geblieben sind. Der mögliche Schaden ist bei den Referenzarchitekturen 2 und 3 am gravierendsten, da hier auf ein zentrales Speichersystem zugegriffen wird.

Risikoindex-Reduzierung nach Umsetzung der Maßnahmen:

Die Umsetzung der „Muss“-Maßnahmen führt, durch die Netzsegmentierung mit VLANs und der Etablierung von vFilern, dazu, dass die Fehlerdomänen sich verkleinern. Das DHCP-Snooping blockiert effektiv Pakete von gespooften IP-Adressen und der Kerberos-Authentifizierungsmechanismus bietet einen Zugriffsschutz auf höherer Protokollebene. Die Eintrittswahrscheinlichkeit und Schadenklasse reduzieren sich somit auf ein unwahrscheinliches und niedriges Maß.

		REF 0	REF 1	REF2	REF 3
	Eintrittswahrscheinlichkeit	Wahrscheinlich	Möglich	Möglich	Möglich
	Schadensklasse	Hoch	Hoch	Sehr hoch	Sehr hoch
Risikoreduzieriung	„Muss“-Maßnahmen:	-7	-4	-4	-4
	„Kann“-Maßnahmen:	-7	-4	-4	-4
NAS - Risiko-index	Nativ	9	6	8	8
	Nach "MUSS"	2	2	2	2
	Nach "KANN"	2	2	2	2

Tabelle 20: Risikobewertung – IP-Address Spoofing

5.5 Risikobewertung für das Zielobjekt „Speicher im Fibre Channel“

Hierbei werden wieder nur die Referenzarchitekturen 1 bis 3 betrachtet, da ein Aufbau in der Referenzarchitektur 0 mit SAN nicht möglich ist.

5.5.1 WWN Spoofing

Eintrittswahrscheinlichkeit:
Aus Wartungsgründen erlauben es die meisten HBA-Hersteller die WWN des HBAs zu verändern. So ist es einem Servicetechniker möglich nach dem Austausch eines defekten HBAs in dem neuem HBA, die WWN des alten HBAs einzutragen. Ein Angreifer der Zugriff auf einen Host hat, der mit dem FC-SAN verbunden ist, kann ohne weiteres die WWN des entsprechenden HBAs anpassen. Der Angriff kann daher als „möglich“ angesehen werden. Es muss aber angemerkt werden, dass für die Aktivierung der neuen WWN gewöhnlich ein Neustarten des Systems erforderlich ist und dies im Allgemeinen nicht unbemerkt bleibt. [FCAn_2006]

Schadenklasse:
Der Schaden, der durch diesen Angriff entstehen kann ist als „hoch“ bzw. „sehr hoch“ zu klassifizieren. Im besten Fall für den Angreifer kann dieser, mit dem Ändern der WWN, den Zugriff auf Ressourcen erlangen, die ihm vorher verwehrt geblieben sind (umgehen von LUN-Masking und Zoning). Der mögliche Schaden ist bei den Referenzarchitekturen 2 und 3 am gravierendsten, da hier auf ein zentrales Speichersystem zugegriffen wird.

Risikoindex-Reduzierung nach Umsetzung der Maßnahmen:
Durch die Einführung der „Muss“-Maßnahme „Port Security“ wird die WWN eines HBA fest mit dem Port eines FC Switches verknüpft. Die Änderung der WWN würde somit zum Ausschluss aus der Fabric führen. WWN Spoofing wäre somit noch möglich, aber die Auswirkungen sinken auf ein „niedriges“ Maß. Die Umsetzung der „Kann“-Maßnahme und die damit einhergehenden Einführung von Authentifizierungsmechanismen, führt in diesem Fall nicht zu einer weiteren Verbesserung des Sicherheitsniveaus.

		REF 0	REF 1	REF2	REF 3
	Eintrittswahrscheinlichkeit		Möglich	Möglich	Möglich
	Schadensklasse		Hoch	Sehr hoch	Sehr hoch
Risikoreduzierung	„Muss“-Maßnahmen:		-6	-6	-6
	„Kann“-Maßnahmen:		-6	-6	-6
SAN - Risiko-index	Nativ		6	8	8
	Nach "MUSS"		2	2	2
	Nach "KANN"		2	2	2

Tabelle 21: Risikobewertung - WWN Spoofing

6 Zusammenfassende Bewertung der unterschiedlichen Konzepte

In diesem Kapitel sollen die unterschiedlichen Referenzarchitekturen in Bezug auf das jeweils betrachtete Speichersystem miteinander verglichen und abschließend bewertet werden.

Grundlage hierfür sind die ermittelten Risikoindizes aus dem vorangegangenen Kapitel „Risikobewertung der einzelnen Gefährdungen“.

Insgesamt wurden 12 Gefährdungen für die NAS-Referenzarchitekturen und 9 Gefährdungen für die SAN-Referenzarchitekturen zusammengetragen.

Wo eine Zuordnung möglich war, wurde der entsprechenden NAS-Gefährdung, die entsprechende SAN-Gefährdung zugewiesen.

Die Zeile „Gesamt“ enthält die Summe der darüber liegenden Risikoindizes.

Die Zeile „Gemittelt“ enthält die gemittelten Werte jeder Spalte.

Hierzu wurde bei den Referenzinfrastrukturen das „Gesamt“-Ergebnis durch die Anzahl an NAS-Gefährdungen geteilt.

Dieses Vorgehen wurde bei der Mittelung der Werte für die SAN-Infrastruktur ebenfalls beibehalten, um dem Umstand Rechnung zu tragen, dass es mehr vorhandene NAS als SAN-Gefährdungen gibt.

Die farbliche Hinterlegung der Einzelbewertungen wurde aus dem vorangegangenen Kapitel übernommen.

Folgende Definition der farblichen Hinterlegung wurde gewählt:

Werte von 1 bis 3:	Gut
Werte von 4 bis 6:	Mittel
Werte größer 6:	Schlecht

Ziel	NAS - Gefährdungen	NAS Referenzarchitektur				SAN Referenzarchitektur			SAN -Gefährdungen
		0	1	2	3	1	2	3	
Server	5.1.1 Virtual Machine Escape	6	6	8	8	6	8	8	5.1.1 Virtual Machine Escape
	5.1.2 Überbuchung von Speicherressourcen	6	6	6	6	6	6	6	5.1.2 Überbuchung von Speicherressourcen
	5.1.3 Fehler im Bandbreitenmanagement	9	6	9	12	6	9	12	5.1.3 Fehler im Bandbreitenmanagement
	5.1.4 Unautorisiertes Mitlesen oder Stören des Virtualisierungsnetzes	12							5.1.4 Unautorisiertes Mitlesen oder Stören des Virtualisierungsnetzes
Switch	5.2.1 MAC Flooding	12	6	6	8				
	5.2.2 MAC Spoofing	9	6	6	8				
	5.2.3 Spanning Tree Angriffe	12	6	6	8	6	6	8	5.3.3 Reconfigure Fabric Attack
	5.2.4 IP Session Hijacking	9	6	6	8	6	6	8	5.3.1 FC Session Hijacking
	5.2.5 Double-Encapsulated 802.1Q Attacke	4	4	4	4				
	5.2.6 ARP Spoofing	9	6	6	8	6	6	8	5.3.2 Name Server Pollution
						8	8	8	5.3.4 E-Port Replication
Speicher	5.4.1 Ausnutzen von "offenen" 802.1Q Trunks	8	6	6	8				
	5.4.2 IP-Adress Spoofing	9	6	8	8	6	8	8	5.5.1 WWN Spoofing
	Gesamt	105	64	71	86	50	57	66	Gesamt
	Gemittelt	**9**	**5**	**6**	**7**	**4**	**5**	**6**	**Gemittelt**

Tabelle 22: Zusammenfassende Risikobewertung vor Maßnahmenumsetzung

Die Tabelle 22 fasst die Ergebnisse der durchgeführten Risikobewertung zusammen.

Hierbei wird ersichtlich, dass die Referenzarchitektur 0 das höchste Gefährdungspotential aufweist. Dies liegt darin begründet, dass Speichernetz und Mandantennetz eine gemeinsame physikalische Infrastruktur benutzen. Es ist wahrscheinlicher, dass es einem internen oder externen Angreifer mit administrativen Rechten auf einem dieser Mandanten möglich ist, einen erfolgreichen Angriff durchzuführen.

Zudem lässt sich aus der Tabelle 22 ersehen, dass mit steigendem Grad der Konsolidierung sich der gemittelte Wert der Risikoindizes verschlechtert. Dies hängt damit zusammen, dass mit einem steigenden Grad der Konsolidierung auch die Auswirkungen von Fehlkonfigurationen und Angriffen steigen. Je mehr Ressourcen konsolidiert werden, umso größer werden die Fehlerdomänen.

Wo es bei der Referenzarchitektur 1 noch für jeden Sicherheitsbereich eigene dedizierte Switche und Speichersysteme gab. Ist dies bei der Referenzarchitektur 3 auf eine gemeinsame Infrastruktur reduziert worden. Auswirkungen oder Unsicherheiten, die bei dieser Referenzarchitektur eine einzelne Komponente betreffen, haben somit Auswirkungen auf alle Sicherheitsniveaus.

In der Gegenüberstellung von SAN und NAS-Speicher, ist aus sicherheitstechnischen Gesichtspunkten ein Vorteil von Fibre-Channel SAN-Systeme zu erkennen. Dies hängt mit der geringeren Anzahl an möglichen Gefährdungen zusammen, die für FC SANs existieren. Im Gegensatz zur Protokollkombination von TCP/IP, ist Fibre Channel aus einem Guss und bietet dementsprechend weniger Angriffsfläche.

OSI	NAS	SAN
Anwendungen	NFS, SMB	FC-4 (Protocol Mapping Layer): SCSI
Darstellung		
Sitzung		FC-3 (Common Services Layer): Verschlüsselung
Transport	TCP, UDP	FC-2 (Network Layer): FC Core
Vermittlung	IP	(kein Äquivalent zur Vermittlungs-schicht)
Sicherung	MAC	FC-3 (Common Services Layer): Verschlüsselung FC-2 (Network Layer): FC Core
Bitübertragung	Ethernet	FC-1 (Data Link Layer): Line Coding FC-0 (Physical): Kabel, Stecker, …

Tabelle 23: Gegenüberstellung NAS / SAN im OSI Modell [FC_2014]

Fibre Channel ist weniger verschachtelt, als es bei TCP/IP der Fall ist. Dies hat nicht nur Vorteile bei der Sicherheit, sondern durch einen geringeren Protokolloverhead auch Vorteile bei der Performance.

Ziel	NAS - Gefährdungen	NAS-Speichersystem Referenzarchitektur				SAN-Speicher Referenzarchitektur			SAN -Gefährdungen
		0	1	2	3	1	2	3	
Server	5.1.1 Virtual Machine Escape	3	3	4	4	3	4	4	5.1.1 Virtual Machine Escape
	5.1.2 Überbuchung von Speicherressourcen	2	2	2	2	2	2	2	5.1.2 Überbuchung von Speicherressourcen
	5.1.3 Fehler im Bandbreitenmanagement	4	4	4	4	4	4	4	5.1.3 Fehler im Bandbreitenmanagement
	5.1.4 Unautorisiertes Mitlesen oder Stören des Virtualisierungsnetzes	4							5.1.4 Unautorisiertes Mitlesen oder Stören des Virtualisierungsnetzes
Switch	5.2.1 MAC Flooding	4	2	2	3				
	5.2.2 MAC Spoofing	3	3	3	3				
	5.2.3 Spanning Tree Angriffe	4	3	3	4	2	2	4	5.3.3 Reconfigure Fabric Attack
	5.2.4 IP Session Hijacking	3	3	3	4	3	3	4	5.3.1 FC Session Hijacking
	5.2.5 Double-Encapsulated 802.1Q Attacke	2	2	2	2				
	5.2.6 ARP Spoofing	2	2	2	2	2	2	2	5.3.2 Name Server Pollution
						4	4	4	5.3.4 E-Port Replication
Speiche	5.4.1 Ausnutzen von "offenen" 802.1Q Trunks	4	3	3	4				
	5.4.2 IP-Adress Spoofing	2	2	2	2	2	2	2	5.5.1 WWN Spoofing
	Gesamt	37	29	30	34	22	23	26	Gesamt
	Gemittelt	**3**	**2**	**3**	**3**	**2**	**2**	**2**	**Gemittelt**

Tabelle 24: Zusammenfassende Risikobewertung nach Umsetzung der „Muss“-Maßnahmen

Die Tabelle 24 stellt die Risikobewertung nach Umsetzung der „Muss“-Maßnahmen dar. Es ist zu erkennen, dass das Sicherheitsniveau des SAN-Speichers, nach Umsetzung aller Maßnahmen, über alle Referenzarchitekturen konstant ist.

Ähnlich verhält sich dies auch beim NAS-Speicher. Einzig die Referenzarchitektur 1 hat hier, Aufgrund ihrer physikalischen Trennung, noch leichte Vorteile, im Gegensatz zu den anderen Architekturmodellen dieser Klasse.

Nach Umsetzung aller Maßnahmen, liegen SAN und NAS in Puncto Sicherheit quasi gleich auf, mit leichten Vorteilen für das SAN.

Ziel	NAS - Gefährdungen	NAS-Speichersystem Referenzarchitektur				SAN-Speicher Referenzarchitektur			SAN -Gefährdungen
		0	1	2	3	1	2	3	
Server	5.1.1 Virtual Machine Escape	3	3	4	4	3	4	4	5.1.1 Virtual Machine Escape
	5.1.2 Überbuchung von Speicherressourcen	1	1	1	1	1	1	1	5.1.2 Überbuchung von Speicherressourcen
	5.1.3 Fehler im Bandbreitenmanagement	4	4	4	4	4	4	4	5.1.3 Fehler im Bandbreitenmanagement
	5.1.4 Unautorisiertes Mitlesen oder Stören des Virtualisierungsnetzes	2							5.1.4 Unautorisiertes Mitlesen oder Stören des Virtualisierungsnetzes
Switch	5.2.1 MAC Flooding	4	2	2	3				
	5.2.2 MAC Spoofing	3	3	3	3				
	5.2.3 Spanning Tree Angriffe	4	3	3	4	2	2	4	5.3.3 Reconfigure Fabric Attack
	5.2.4 IP Session Hijacking	3	3	3	4	3	3	4	5.3.1 FC Session Hijacking
	5.2.5 Double-Encapsulated 802.1Q Attacke	2	2	2	2				
	5.2.6 ARP Spoofing	2	2	2	2	2	2	2	5.3.2 Name Server Pollution
						4	4	4	5.3.4 E-Port Replication
Speiche	5.4.1 Ausnutzen von "offenen" 802.1Q Trunks	4	3	3	4				
	5.4.2 IP-Adress Spoofing	2	2	2	2	2	2	2	5.5.1 WWN Spoofing
	Gesamt	34	28	29	33	21	22	25	*Gesamt*
	Gemittelt	**3**	**2**	**2**	**3**	**2**	**2**	**2**	**Gemittelt**

Tabelle 25: Zusammenfassende Risikobewertung nach Umsetzung der „Kann“-Maßnahmen

Nach Umsetzung der „Muss“-Maßnahmen ist bereits ein so hohes Sicherheitsniveau erreicht worden, dass keine signifikante Steigerung des allgemeinen Sicherheitsniveaus mehr zu verzeichnen ist.

Die Umsetzung einzelner „Kann“-Maßnahmen ist aber zur Erhöhung des Schutzgrades im Einzelfall möglich.

7 Referenzkonfigurationen zur Speicheranbindung für höchste Sicherheitsanforderungen

In diesem Kapitel wird die Referenzkonfiguration zur Speicheranbindung für höchste Sicherheitsanforderungen beschrieben. Dabei sind die Erkenntnisse der vorangegangenen Kapitel die Grundlage dieses Kapitels.

Es werden die zuvor ermittelten Maßnahmen für Network Attached Storage und Storage Area Networks zu einem Best-Practice zusammengefasst und exemplarisch an Beispielarchitekturen dargestellt.

Die dargestellten Lösungen beziehen sich hierbei auf die Verwendung der Referenzarchitektur 3.

7.1 Lösung für NAS

Fasst man alle zuvor definierte Maßnahmen für NAS zusammen, ergibt sich folgende Liste an Maßnahmen zur Implementierung einer Lösung für Speicheranbindung mit höchsten Sicherheitsanforderungen.

M 4.2.1.1	Einsatz von Port Security auf Netzwerkswitchen
M 4.2.3.1	Konfiguration von Root und BPDU Guard
M 4.2.3.2	Die Root Bridge manuell festlegen
M 4.2.4.1	Nutzung von IPsec
M 4.2.5.1	Entfernen des nativen VLANs von allen Access-Ports
M 4.2.5.2	Festlegen eines ungenutzten VLANs als natives VLAN für alle Trunks
M 4.2.6.2	Einsatz von DHCP Snooping
M 4.2.6.3	Einsatz von VLAN
M 4.4.2.2	Nutzung von vFilern und VLANs
M 4.4.2.3	Implementierung von Kerberos Authentication Mechanismen
M 4.5.1.4	Verschlüsselung der abgelegten Daten

Tabelle 26: Zusammengefasste Maßnahmen im Bereich NAS

Die Abbildung 43 stellt die aus den Maßnahmen abgeleitete Sicherheitsarchitektur für NAS dar.

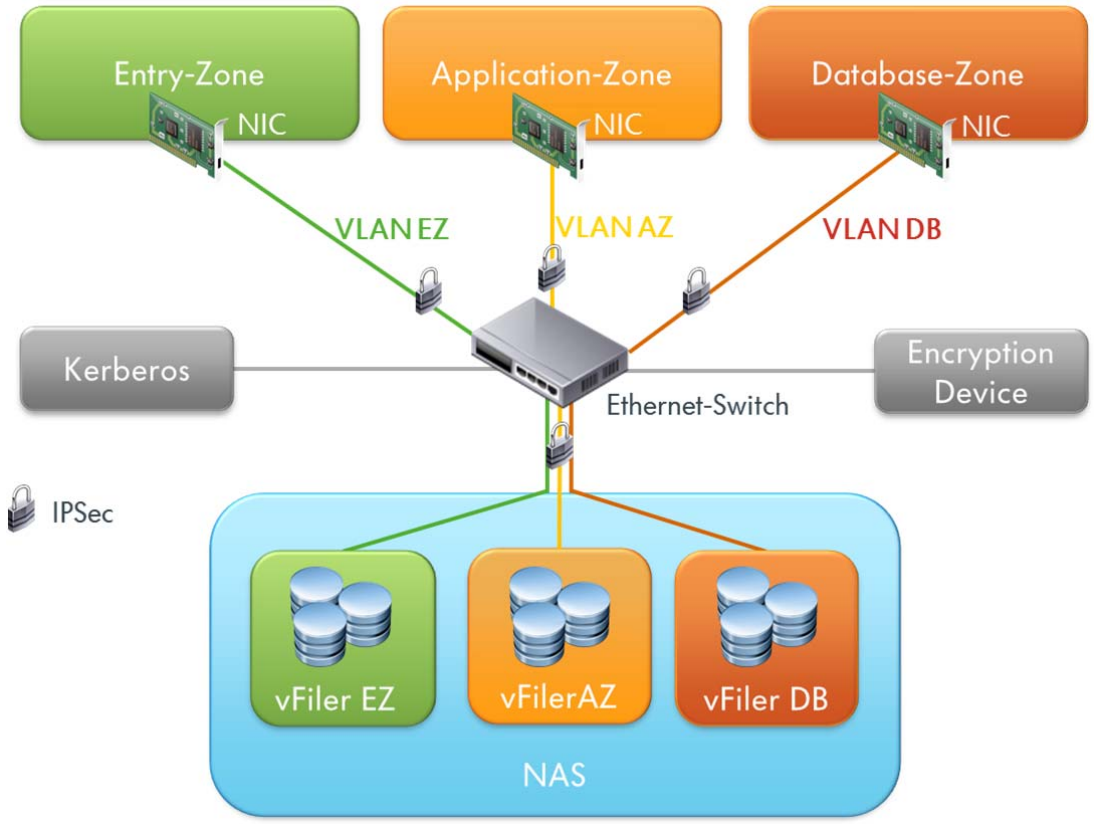

Abbildung 43: Sicherheitsarchitektur NAS

Auf dem Ethernet-Switch wurden die Sicherheitsfeatures Port-Security, DHCP Snooping, Root und BPDU Guard aktiviert. Die Root-Bridge wurde festgelegt (auf dieser Abbildung nicht dargestellt). Die Kommunikationsverbindungen werden, Ende-zu-Ende, mit IPsec verschlüsselt. Die VLANs wurden entsprechend den Maßnahmen vergeben. Hierbei wird für jeden Sicherheitsbereich mindestens ein VLAN vorgesehen. Zudem verfügt jeder Sicherheitsbereich über einen eigenen vFiler. Die Netzwerkdateisysteme nutzen zur Authentifizierung Kerberos und die Daten werden mittels eines Encryption Devices verschlüsselt abgelegt.

7.2 Lösung für SAN

Fasst man alle zuvor definierte Maßnahmen für SAN zusammen, ergibt sich folgende Liste an Maßnahmen zur Implementierung einer Lösung für Speicheranbindung mit höchsten Sicherheitsanforderungen.

M 4.3.1.1	Nutzung von FCsec
M 4.3.2.1	Nutzung von Authentifizierungsmechanismen am Name Server
M 4.3.2.2	Verwendung von vSAN
M 4.5.1.2	Verwendung von Port-Based Hard-Zoning
M 4.3.3.2	Unterdrücken von RSCNs Nachrichten auf Switch-Ebene
M 4.3.4.1	Absicherung unbenutzter Ports
M 4.3.4.2	Verwendung von Port Type Locking
M 4.5.1.1	Verwendung von Physical Port Locking
M 4.5.1.3	Abweisen doppelter WWNs
M 4.5.1.4	Verschlüsselung der abgelegten Daten
M 4.5.1.5	LUN-Masking

Tabelle 27: Zusammengefasste Maßnahmen im Bereich SAN

Die Abbildung 44 stellt die aus den Maßnahmen abgeleitete Sicherheitsarchitektur für SAN dar.

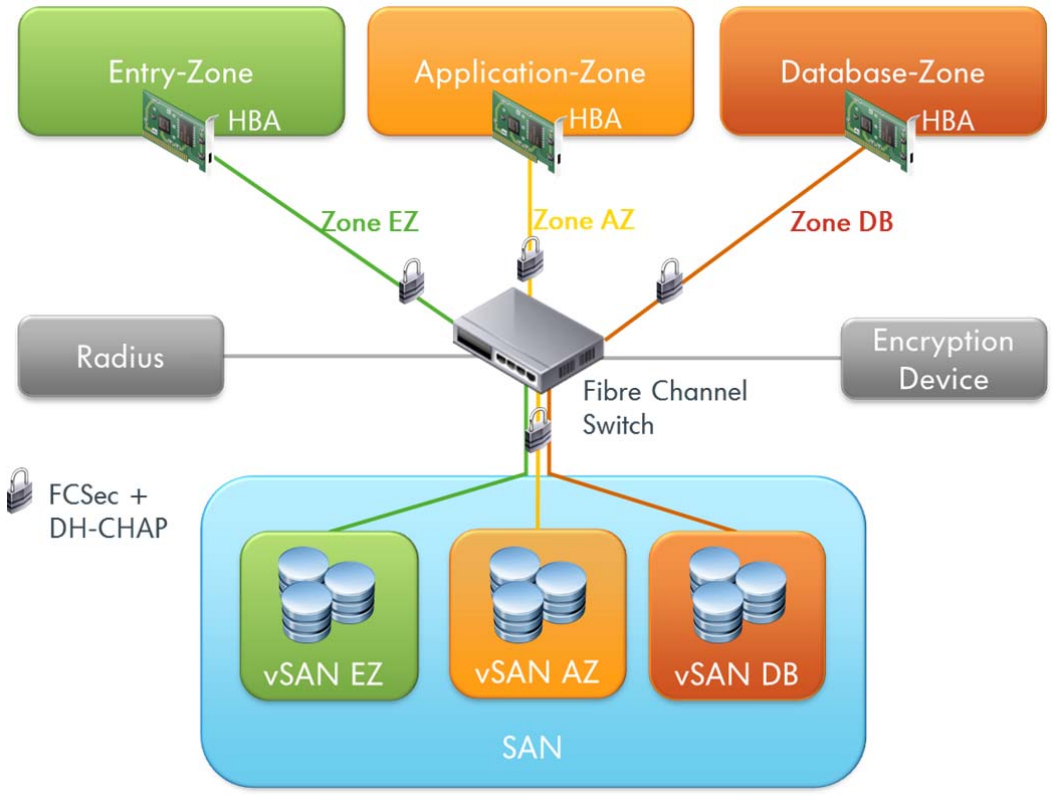

Abbildung 44: Sicherheitsarchitektur SAN

Auf dem FC-Switch wurden die Sicherheitsfeatures des Abweisens doppelter WWNs, Physical Port Locking, Port Type Locking und Unterdrückung von RSCNs Nachrichten aktiviert. Die Kommunikationsverbindungen werden, Ende-zu-Ende, mit FCsec verschlüsselt. Für jeden Sicherheitsbereich wird mindestens eine Zone vorgesehen. Hierbei wird port-basiertes Hard-Zoning verwendet. Zudem verfügt jeder Sicherheitsbereich über ein eigenes vSAN. Zur Authentifizierung wird DH-CHAP, welches auf einen Radius-Server zugreift, verwendet und die Daten werden mittels eines Encryption Devices verschlüsselt abgelegt und mittels LUN-Masking vor unberechtigten Zugriffen geschützt.

8 Ergebnisse und Ausblick

Die gewonnenen Ergebnisse werden im abschließenden Kapitel zusammengefasst und die Weiterentwicklungspotenziale aufgezeigt.

8.1 Ergebnisse

Das Diplomarbeitsthema „Sicherheitstechnische Betrachtung von Speichernetzen im Bereich der Servervirtualisierung und segmentierten Netzen“ ergab sich aus der Anforderung der Volkswagen IS Security Organisation (ISSO) ein Konzept für die zentrale Speicher-Infrastruktur zu erstellen.

Hierzu sollte abhängig von der Sicherheitsklasse festgelegt werden, welche Maßnahmen hinsichtlich der Authentifizierung und der Verschlüsselung bei der Nutzung von Speichersystemen und Speichernetzen notwendig sind.

Das Kapitel 4 hat hierzu die Maßnahmen definiert und als Ergebnis hat das Kapitel 7 diese Maßnahmen übersichtlich, in tabellarischer Form zusammengefasst.

Die VW ISSO hat die Empfehlung ausgesprochen für die Virtualisierungshosts SAN-basierten Speicher zu verwenden. Hingegen dieser Empfehlung konnte in Kapitel 6 festgestellt werden, dass es mit Umsetzung aller „Muss“-Maßnahmen möglich ist, sowohl bei SAN und NAS ein ähnliches Sicherheitsniveau zu erreichen und das quasi unabhängig von der Referenzarchitektur.

8.2 Ausblick

Die Aufrechterhaltung der Informationssicherheit ist ein kontinuierlicher Prozess, neue Entwicklungen und Erkenntnisse führen zu einer stetigen Veränderung. So hat der Heartbleed-Bug[19] Anfang 2014 schmerzlich vor Augen geführt, dass selbst Techniken, die die Informationssicherheit erhöhen sollen, fehlerhaft sein können.

Wie schon in der Einleitung beschrieben hat die Anzahl der Angriffe aus dem Internet in den letzten Jahren stetig zugenommen. Die Delikte, die Datenveränderung und Computersabotage betreffen, haben sich in den letzten vier Jahren mehr als verfünffacht. Allein in 2013 wurden laut dem „Symantec – Internet Security Threat Report“ über 6787 Ver-

[19] Der Heartbleed-Bug ist ein schwerwiegender Programmfehler in älteren Versionen der Open-Source-Bibliothek OpenSSL, durch den über verschlüsselte TLS-Verbindungen private Daten von Clients und Servern ausgelesen werden können. [HeBl_2014]

wundbarkeiten identifiziert. Dies ist der höchste Stand seit der Erhebung in 2006. [ISTR_2014]. Das Gefährdungspotential bleibt konstant hoch.

Ob das derzeitige Sicherheitsniveau noch gehalten wird, muss daher fortlaufend geprüft werden und je nach Ergebnis gehandelt werden.

Auch die Konzepte zur Speicheranbindung können mit der Zeit Änderungen unterworfen sein. Im Kapitel „Abgrenzung der Aufgabenstellung“ wurde hier unter Anderem iSCSI SAN genannt das eine immer größere Verbreitung erfährt. Zudem muss erwähnt werden, dass Implementierungen, basierend auf lokalem Speicher in einem verteilten Dateisystem, sich aktuell in der Entwicklung befinden (z.B. vSphere 5.5 vSAN-Feature) und in diesem Bereich DAS zukünftig wieder eine verstärkte Bedeutung erlangen könnte. Die Verlagerung des Speichers „wieder“ in die Server hätte sowohl neue organisatorische als auch technische Herausforderungen.

Index

Literatur

[Bitk2009] BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.: Server-Virtualisierung. URL: < http://www.bitkom.org/de/publikationen/38337_40545.aspx >, verfügbar am 03.05.2013

[BSI2011] Bundesamt für Sicherheit in der Informationstechnik: G 2.148 Fehlerhafte Planung der Virtualisierung. URL: < https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g02/g02148.html >, verfügbar am 03.05.2013

[Schm2009] Prof. Dr. Dipl.-Ing. Wilfried Schmalwasser: Speichernetzwerke, , URL: < https://www.staff.hs-mittweida.de/~ws/intranet/PCT/Lehrunterlagen/SAN_NAS.pdf >, verfügbar am 03.05.2013

[VMWa2012] Dennis Zimmer, Bertram Wöhrmann, Carsten Schäfer, Günter Baumgart, Oliver Kügow, Urs Stephan Alder, Marcel Brunner: VMware vSphere 5, Galileo Computing, 2012

[TDas2013] Andreas Wurm; Speichernetze mit NAS und SAN; URL: < http://www.tecchannel.de/bild-zoom/445645/3/349890/il-75775276497896038/>; verfügbar am 11.05.2013

[Spe2008] Speichernetze; Ulf Troppens, Rainer Erkens, Wolfgang Müller; d. Punkt Verlag, ISBN-978-3-89864-393-1

[Ga2012] John Monroe; Market Share Analysis: Network-Attached Storage and Unified Storage, Worldwide, 2012; URL: < http://www.gartner.com/technology/reprints.do?id=1-1GUZA31&ct=130703&st=sb >, verfügbar am 26.10.2013

[GMaQ2013] Latest Gartner Magic Quadrant Positions VMware in Leaders Quadrant for x86 Server Virtualization Infrastructure; Veröffentlich am: 11.07.2013; URL: < http://blogs.vmware.com/vmware/2013/07/vmware-leader-2013-gartner-magic-quadrant-server-virtualization.html >; verfügbar am: 07.11.2013

[x86w2013] x86-Prozessor; URL: < http://de.wikipedia.org/wiki/X86-Prozessor >; verfügbar am: 07.11.2013

[GaSv2007] Server Virtualization Can Break DMZ Security; URL: < https://www.gartner.com/doc/506381/server-virtualization-break-dmz-security >; verfügbar am: 23.02.2013

[VMWa2014] VMware, DMZ Virtualization with VMware Infrastructure, URL: < http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1008076 >; verfügbar am: 18.04.2014

[WsSs2104] Dieter Fiegert; Wie sicher sind Storage Networks?; URL: <

http://www.computerwoche.de/a/wie-sicher-sind-storage-networks,550579 >; verfügbar am: 29.04.2014

[DeIn2003] Dell Storage Consolidation; URL: < http://www.dell.com/downloads/global/products/pvaul/en/storage_consol.pdf > ;verfügbar am: 02.06.2014

[CSSE2011] Gefährdungen und Gegenmaßnahmen beim Einsatz von VCE Vblock; Version 2.5; Stephan Bohnengel, Klaus Böttcher, Dr. Clemens Doubrava Alex Didier Essoh, Yves Fauser, Isabel Münch, Norbert Olbrich, Michael Otto, Gerald Pernack, Wolfgang Reh; 22. Dez. 2011

[BSI2014] Bundesamt für Sicherheit in der Informationstechnik; Band B, Kapitel 6: Speichertechnologien; URL: < https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Hochverfuegbarkeit/BandB/B6_Speicher.pdf?__blob=publicationFile >; verfügbar am 04.06.2014

[Sec2005] Securing Storage: A Practical Guide to SAN and NAS Security; Himanshu Dwivedi; Addison-Wesley Professional; ISBN: 978-0321885746

[Sto2003] Präsentation – Storage Security; Himanshu ecuring Storage: A Pr; Blackhat; 2003; URL: < http://www.blackhat.com/presentations/bh-usa-03/bh-us-03-dwivedi.pdf >; verfügbar am: 13.06.2014

[TdI2007] Taschenbuch der Informatik; Uwe Schneider, Dieter Werner; Carl Hanser Verlag; ISBN: 978.3.446-40754-1

[Int12012] Internet (1), Aufbau, Adressierung, Betrieb; Prof. Dr.-Ing. habil. Lutz Winkler; Hochschule Mittweida; Version: 2012-04

[Int22012] Internet (2), Transportdienste und Protokolle; Prof. Dr.-Ing. habil. Lutz Winkler; Hochschule Mittweida; Version: 2011-12

[BSI_1002] Bundesamt für Sicherheit in der Informationstechnik; BSI-Standard 100-3 Risikoanalyse auf Basis von IT-Grundschutz; URL: < http://www.bsi.bund.de/gshb >; Version 2.5; Verfügbar am: 21.60.2014

[B_Virt3304] Bundesamt für Sicherheit in der Informationstechnik; B 3.304 Virtualisierung; ULR: < https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b03/b03304.html >; Stand: 12. EL Stand 2011; Verfügbar am: 22.06.2014

[Res_G477] Bundesamt für Sicherheit in der Informationstechnik; G 4.77 Ressourcenengpässe durch fehlerhafte Funktion der Gastwerkzeuge in virtuellen Umgebungen; ULR: < https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g04/g04077.html >; Stand: 12. EL Stand 2011; Verfügbar am: 23.06.2014

[SiKo_M4346] Bundesamt für Sicherheit in der Informationstechnik; M 4.346 Sichere Konfiguration virtueller IT-Systeme; URL: < https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04346.html >, Stand: 12.

EL Stand 2011; verfügbar am: 23.07.2014

[Una_G5147] Bundesamt für Sicherheit in der Informationstechnik; G 5.147 Unautorisiertes Mitlesen oder Stören des Virtualisierungsnetzes; URL: < https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g05/g05147.html >; Stand: 12. EL Stand 2011; Verfügbar am: 24.06.2014

[RuS_B3302] Bundesamt für Sicherheit in der Informationstechnik; B 3.302 Router und Switches; URL: < https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b03/b03302.html >; Stand: 11. EL Stand 2009; Verfügbar am: 25.06.2014

[VSWP_2014] Cisco; VLAN Security White Paper; URL: < http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a008013159f.shtml#wp39054 >; verfügbar am: 25.06.2014

[NW_2007] Network Warrior; Gary A. Donahue; O' Reilly Media Inc.; ISBN: 978-0-596-10151-0

[BpfSN2007] Best Practices for Storage Networks; George G. Meade; National Security Agency, URL: < http://www.nsa.gov/ia/_files/vtechrep/I732-012R-2007.pdf >Stand: 18.10.2007; Verfügbar am: 25.06.2014

[CoSa_2013] Computersabotage; Wikipedia; URL: < http://de.wikipedia.org/wiki/Computersabotage >; verfügbar am 26.06.14

[ISRM_2011] Information Security Risk Management; Sebastian Klipper; Vieweg+Teubner Verlag; ISBN 978-3-8348-1360-2

[vSHG_2013] vSphere 5.5 Security Hardening Guide; VMware; URL: < https://communities.vmware.com/thread/461706 >Stand: 30.10.2013

[AvGt_2009] A VMware Guest to Host Escape Story; Kostya Kortchinsky; Immunity, Inc.; BlackHat USA 2009, Las Vegas; URL: < http://www.blackhat.com/presentations/bh-usa-09/KORTCHINSKY/BHUSA09-Kortchinsky-Cloudburst-SLIDES.pdf > ; verfügbar am: 08.07.2014

[vSSp_5_1] vSphere-Speicher ESXi 5.1 vCenter Server 5.1, VMWare; URL: < http://ts-vm.de/index.php/downloads/category/17-esxi-und-vcenter?download=154:vsphere-esxi-vcenter-server-51-storage-guide >, verfügbar am: 23.07.2014

[OpSc_2012] VMware vSphere: Optimize and Scale – Lecture Manual – Volume 1; VMware; Lecture Manual – Volume 1, Revision A, Part Number EDU-EN-OS51_LECT1

[VVNC_2007] VMware Virtual Networking Concepts; VMware; URL: < http://www.vmware.com/files/pdf/virtual_networking_concepts.pdf >; Revision: 20070718 Item: IN-018-INF-01-01; verfügbar am: 24.07.2014

[MacF_2013] MAC-Flooding; Wikipedia; URL: < http://de.wikipedia.org/wiki/MAC-Flooding >; Stand: 25. März 2013 um 17:55; verfügbar am: 25.07.2014

[PoSe_2013] Port Security; Wikipedia; URL: < http://de.wikipedia.org/wiki/Port_Security >; Stand: 3. Februar 2013 um 16:44 Uhr; verfügbar am: 25.07.2014

[EiVL_2006] Einführung in VLANs, Teil 1; Cisco Systems, URL: < http://www.tecchannel.de/netzwerk/lan/434093/einfuehrung_in_vlans_teil_1/index5.html >; Stand: 17.03.2006; verfügbar am: 26.07.2014

[VLan_2013] VLANS, Basant Shrestha; URL: <http://basantshrestha.wordpres.com/2013/02/04/vlan/ >; Stand: 04.02.2013; verfügbar am: 26.07.2014

[IERa_2014] IEEE 802.1x / RADIUS; Elektronik Kompendium; URL: < http://www.elektronik-kompendium.de/sites/net/1409281.htm >; verfügbar am: 26.07.2014

[IE802x_2014] IEEE 802.1X; Wikipedia; URL: < http://de.wikipedia.org/wiki/IEEE_802.1X >; verfügbar am: 26.07.2014

[SHAS_2012] Switches and Hubs and Security Oh my!; Bradley Graham; URL: < https://learningnetwork.cisco.com/blogs/journey-back-to-ccna/2012/02/16/switches-and-hubs-and-security-oh-my >; Stand: 16.02.2012 09:01:52; verfügbar am: 26.07.2014

[Broc_2014] Broadcast; Wikipedia; URL: < http://de.wikipedia.org/wiki/Broadcast >; Stand: 01.06.2014 14:14 Uhr; verfügbar: 26.07.2014

[L2AM_2012] Layer 2 Attacks – MAC Address Spoofing Attacks; y Jinshu Peethambaran; Secure Leaves; URL: < http://secureleaves.com/2012/11/05/layer-2-attacks-mac-address-spoofing-attacks/ >; Stand: 05.011.2012; verfügbar am: 26.07.2014

[LANS_2004] LAN-Sicherheit; Andreas Aurand; dPunkt Verlag; ISBN: ISBN: 978-3-89864-297-2; Stand: September 2004

[PtCC_2014] Protecting the Cisco Catalyst 6500 Series Switches Against Denial-Of-Service Attacks; Cisco; URL: < http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/prod_white_paper0900aecd802ca5d6.html >; verfügbar am: 26.07.2014

[DHCPSn12] DHCP snooping; Wikipedia; URL: < http://en.wikipedia.org/wiki/DHCP_snooping >; verfügbar: 26.07.2014

[IPSecE2014] IPsec - Security Architecture for IP; Elektronik Kompendium; URL: < http://www.elektronik-kompendium.de/sites/net/0906191.htm >; verfügbar am: 28.07.2014

[VPNs_2014] VPNs mit IPsec; FreeBSD; URL: < http://www.freebsd.org/doc/de/books/handbook/ipsec.html >; verfügbar am: 28.07.2014

[FCSp_2014] FC-SP, fibre channel security; speicherguide.de Das Storage Magazin; URL: < http://www.speicherguide.de/wissen/glossar/f/fc-sp,-fibre-channel-security-protocol-8173.aspx >; verfügbar am: 29.07.2014

[DHCh_2014] FC-SP and DHCHAP; Cisco; URL: < http://www.cisco.com/en/US/docs/storage/san_switches/mds9000/sw/rel_2_x/fm/configuration/guide/fcsp.html >; Stand: Cisco MDS 9000 Family Fabric Manager Configuration Guide, Release 2.x; verfügbar am: 30.07.2014

[SFCN_2014] Securing Fibre Channel Storage Area Networks; Systems and Network Analysis Center (SNAC); URL :< http://www.nsa.gov/ia/_files/factsheets/securing_fibre_brochure.pdf >; Stand: NSA Creative Imaging 30684; verfügbar am: 30.07.2014

[FCDH_2003] FC-SP DH-CHAP Specification; Claudio DeSanti, Larry Hofer, Fabio Maino; URL:< ftp://ftp.t10.org/t11/document.03/03-047v0.pdf >; Stand: DH-CHAP Specification, 03-047v0, January 2003; verfügbar am: 30.07.2014

[FCSp_2004] FC-SP Architecture, Claudio DeSanti; URL:< ftp://ftp.t10.org/t11/document.04/04-272v0.pdf >; Stand: 04-272v0, April 2004; verfügbar am: 31.07.2014

[FCPap_2002] FCPAP: Fibre Channel Password Authentication and Key Exchange Protocol; Claudio DeSanti, Fabio Maino; Andiamo Systems, Inc.; URL: < ftp://ftp.t10.org/t11/document.02/02-512v1.pdf >; Stand: T11/02-512v1; verfügbar am: 03.08.2014

[FCAn_2006] Fibre Channel Storage Area Networks: An Analysis From A Security Perspective; SANS Institute; José Picó, URL: < http://www.sans.org/reading-room/whitepapers/backup/fibre-channel-storage-area-networks-analysis-security-perspective-32913 >; Stand: March 14th 2006; verfügbar am: 03.08.2014

[ISMH_2004] Information Security Management Handbook, Vol. 2; Harold F. Tipton, Micki Krause; Auerbach Publications; Stand: 28.12.2004; ISBN-13: 978-0203005552

[NOSA_2014] Network OS Administrator's Guide, Zoning overview; Brocade; URL:< http://www.brocade.com/downloads/documents/html_product_manuals/NOS_AG_300/wwhelp/wwhimpl/common/html/wwhelp.htm#context=53_1002561_02&file=CH_zoning.13.02.html >; Stand: Network OS v3.0.0 53-1002561-02; verfügbar am: 03.08.2014

[IPSp_2014] IP spoofing; Wikipedia; URL: < http://de.wikipedia.org/wiki/IP-Spoofing >; Stand: 2. September 2013, 00:07 Uhr; verfügbar am: 04.08.201^4

[ARP_2010] Using Dynamic ARP Inspection; Marcus V Morais; URL:< http://bi0os.blogspot.de/2010/05/using-dynamic-arp-inspection.html >Stand: 16 May 2010; verfügbar am: 05.08.2014

[vSAN_2014] Configuring and Managing VSANs; Cisco; URL:< http://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/4_1/configuration/guides/cli_4_1/clibook/vsan.html >; verfügbar am: 06.08.2014

[VL_G_2014] VLAN Grundlagen; Werner Fischer; Fa. Thomas Krenn; URL: < http://www.thomas-krenn.com/de/wiki/VLAN_Grundlagen >; verfügbar am: 06.08.2014

[vFil_2009] Site Recovery Manager: It's Not Just for VMs; Vaughn Stewart; URL: < http://purestorageguy.com/2009/04/17/site-recovery-manager-its-not-just-for-vms/ >; Stand: 17.04.2009; verfügbar am: 06.08.2014

[Yers_2005] Yersinia; David Barroso, Alfredo Andres; Blackhat EU 2005; URL:< http://www.blackhat.com/presentations/bh-europe-05/BH_EU_05-Berrueta_Andres/BH_EU_05_Berrueta_Andres.pdf >; verfügbar am: 07.08.2014

[FC_2014] FibreChannel; Wikipedia; URL:< http://de.wikipedia.org/wiki/Fibre_Channel >; verfügbar am: 09.08.2014

[SfIS_2014] 4.4 Schutzbedarfsfeststellung für die IT-Systeme; Bundesamt für Sicherheit in der Informationstechnik; URL:< https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/WebkursITGrundschutz/Schutzbedarfsfeststellung/ITSysteme/itsysteme_node.html >; verfügbar am: 13.08.2014

[SuSz_2014] 4.2.3 Schutzbedarf und Schutzziele; Bundesamt für Sicherheit in der Informationstechnik; URL:< https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/WebkursITGrundschutz/Schutzbedarfsfeststellung/Schutzbedarfskategorien/Schutzziele/schutzziele_node.html >; verfügbar am: 13.08.2014

[AeAW_2014] M 4.176 Auswahl einer Authentisierungsmethode für Webangebote; Bundesamt für Sicherheit in der Informationstechnik; URL:< https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04176.html >; verfügbar am: 13.08.2014

[HeBl_2014] Heartbleed; Wikipedia; URL:< http://de.wikipedia.org/wiki/Heartbleed >; verfügbar am: 15.08.2014

[ISTR_2014] Internet Security Threat Report; Symantec; URL: < http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_appendices_v19_221284438.en-us.pdf >; Stand: Vol-

ume 19; verfügbar am: 15.08.2014

[CVS_2014] Common Vulnerabilities and Exposures; Wikipedia; URL:< http://de.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures >; Stand: 10.04.2014; verfügbar am: 16.08.2014

[WuAm_2014] Wahrscheinlichkeits- und Auswirkungsmatrix; Tom Alby, David Braun, Sabine Pfleger; InLoox GmbH; URL: < http://projektmanagement-definitionen.de/impressum/ >; verfügbar am: 30.06.2014

[SANS_2014] SANS; Wikipedia; URL:< http://de.wikipedia.org/wiki/SANS >, verfügbar am: 17.08.2014

.

Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe.

Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht.

Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt.

Wolfsburg, den 19.08.2014

Roman Wolf